**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND**

| | |
|---|---|
| IN RE: MARRIOTT INTERNATIONAL, INC., CUSTOMER DATA SECURITY BREACH LITIGATION | MDL No. 19-md-2879<br><br>Judge Paul W. Grimm |
| This Document Relates To:<br><br>JOHN P. MOORE, Derivatively on Behalf of MARRIOTT INTERNATIONAL, INC.,<br><br>Plaintiff,<br><br>vs.<br><br>J.W. MARRIOTT, JR., MARY K. BUSH, BRUCE W. DUNCAN, DEBORAH M. HARRISON, FREDERICK A. HENDERSON, ERIC HIPPEAU, LAWRENCE W. KELLNER, DEBRA L. LEE, AYLWIN B. LEWIS, GEORGE MUÑOZ, STEVEN S. REINEMUND, SUSAN C. SCHWAB, and ARNE M. SORENSON,<br><br>Defendants,<br><br>and,<br><br>MARRIOTT INTERNATIONAL, INC.,<br><br>Nominal Defendant. | This document relates to Case Nos: 8:19-cv-00830- PWG and 8:19-cv-00812-PWG<br><br>**JURY TRIAL DEMANDED** |

*Caption continued on next page*

EDMUND ALVES, Derivatively on Behalf of MARRIOTT INTERNATIONAL, INC.,

Plaintiff,

vs.

ARNE M. SORENSON, KATHLEEN KELLY OBERG, BAO GIANG VAL BAUDUIN, BRUCE HOFFMEISTER, J.W. MARRIOTT, JR., BRUCE W. DUNCAN, DEBORAH MARRIOTT HARRISON, FREDERICK A. HENDERSON, ERIC HIPPEAU, LAWRENCE W. KELLNER, DEBRA L. LEE, AYLWIN B. LEWIS, GEORGE MUÑOZ, STEVEN S REINEMUND, and SUSAN C. SCHWAB,

Defendants,

and

MARRIOTT INTERNATIONAL, INC.,

Nominal Defendant.

**VERIFIED SHAREHOLDER DERIVATIVE**
**SECOND AMENDED CONSOLIDATED COMPLAINT**

# TABLE OF CONTENTS

Plaintiffs Edmund Alves and John P. Moore (collectively, "Plaintiffs"), by and through their undersigned counsel, derivatively on behalf of Nominal Defendant Marriott International, Inc. ("Marriott" or the "Company"), submit this Verified Shareholder Derivative Second Amended Consolidated Complaint (the "Complaint"). Plaintiffs' allegations are based upon their personal knowledge as to themselves and their own acts, and upon information and belief, developed from the investigation and analysis by Plaintiffs' counsel, including a review of publicly available information, including filings by Marriott with the U.S. Securities and Exchange Commission ("SEC"), press releases, news reports, analyst reports, investor conference transcripts, publicly available filings in lawsuits, a review and analysis of a confidential forensic report commissioned by Marriott following the Data Breach (the "PFI Report") that is the subject of this litigation)[1], a review of pleadings and exhibits filed in other state and federal litigation arising out of the data breach that is the subject of this litigation (the "Data Breach") and matters of public record.

## I. NATURE OF THE ACTION

1. This is a shareholder derivative action brought in the right, and for the benefit, of Marriott against certain of its officers and directors seeking to remedy the damages caused by the Director Defendants and Officer Defendants (defined below) for breach of fiduciary duties, corporate waste, unjust enrichment, violations of Section 10(b) of the Exchange Act and SEC Rule

[1] Plaintiffs' counsel fought to have the PFI Report publicly unsealed after a sealed version was filed on the public docket. Following a data breach, a compromised company must hire a Payment Card Industry Forensic Investigator ("PFI"). The PFI conducts a forensic investigation and writes a report detailing its investigation, the PFI Report. If the investigation finds evidence of a data breach, the report explains how the attack was carried out. Marriott hired Verizon to conduct a forensic investigation into the Data Breach. Verizon conducted an investigation and authored a report detailing its industry-standard investigation and findings in the PFI Report. The findings of this report are discussed in detail herein, and a copy of the PFI Report is attached hereto as Exhibit A.

10b-5, and violations of Sections 14(a) and 20(a) of the Exchange Act that occurred from November 16, 2015 to the present ("Relevant Period"), and which has caused substantial harm to Marriott.

2. This derivative action arises from Marriott's acquisition of Starwood Hotels and Resorts Worldwide, Inc. ("Starwood") in 2016 and a data breach suffered by Starwood which began in 2014 and remained undiscovered by Marriott until 2018.

3. Marriott operates, franchises, and licenses hotel, residential, and timeshare properties worldwide. Starwood has described itself as a hotel and leisure company, with hotel brands that include the W Hotels, St. Regis, and Le Meridien.

4. On November 16, 2015, Marriott and Starwood announced their plan to merge Starwood into Marriott creating the world's largest hotel company (the "Merger"). On September 23, 2016, Marriott announced that this Merger was completed.

5. However, unbeknownst to Marriott's customers, investors, and the public at large, in July 2014, computer hacker(s) (the "Hackers") took advantage of vulnerabilities in the Starwood network to install malicious software. From that date and continuing until September 2018 (which included the period of the Merger) and using this software, the Hackers had copied and encrypted information from the Starwood guest reservation database, which database was part of the assets acquired by Marriott in the Merger. The information included some combination of names, mailing addresses, phone numbers, email addresses, passport numbers, Starwood Preferred Guest ("SPG") account information, dates of birth, gender, arrival and departure information, reservation dates, communication preferences, payment card numbers, payment card expiration dates, and tools needed to decrypt cardholder data.

6. During Marriott's Merger due diligence and post-Merger integration process,

Defendants (defined below) repeatedly assured investors that Marriott performed adequate due diligence, planned for and dedicated adequate resources to the integration of the two companies (the "Integration"), and that Defendants' prior experience with much smaller acquisitions prepared them for the acquisition of Starwood. As the Company's purported due diligence efforts proceeded, Defendants' representations about Marriott's "extensive" and "exhaustive" diligence efforts became more and more definitive. These representations included statements maintaining that Marriott's Board of Directors (the "Board") was continually apprised of the due diligence process. Indeed, the Board was provided three presentations, at least, on cybersecurity risks by the Company's Chief Financial Officer ("CFO") during the Relevant Period. Moreover, Defendants also falsely represented that Starwood's prized customer data was protected by various safeguards and security measures.

7. In fact, Defendants failed in their due diligence obligations relating to cybersecurity risks at Starwood and in its information technology ("IT") systems (either directly as officers or through a failure of oversight by the Board) and based thereon knew, or were at least reckless in not knowing, of the deficiencies in Starwood's cybersecurity practices and IT systems, and related risks. The Board and the Company's management became aware of the security vulnerabilities in Starwood's systems after the acquisition—yet, chose to maintain the existing outdated system rather than upgrade those systems—which themselves were not only outdated but failed to meet industry standards. Notably, Starwood's IT and security systems were so blatantly insecure and outdated, that even a perfunctory review of them would have revealed their deficiencies and rampant vulnerabilities. In January 2017, the Company's consultant, PricewaterhouseCoopers ("PwC") presented an assessment on Starwood's cybersecurity, which detailed significant issues with Starwood's security systems. Defendants were also informed about Marriott's own security

weaknesses and Starwood's noncompliance with mandated standards for managing credit card data as of February 2017, at least, when the Board and certain other defendants were specifically informed of such information and related risks stemming therefrom. PwC also conducted an assessment in the middle of that same year over the Integration of Starwood and Marriott and provided Defendants with remediation activities to address issues with the combined network. Among these remediation activities was two-factor authentication. However, Defendants failed to take any action, leaving Starwood's system and the customer data on that system vulnerable.

8. On November 30, 2018, Marriott issued a press release revealing a "data security incident" involving the Starwood guest reservation database, which had been discovered upon investigating a September 8, 2018 internal security alert. As discussed in the press release, Marriott believed the impacted Starwood guest reservation database contained information on up to approximately 500 million guests who made a reservation at a Starwood property. In its January 4, 2019 update press release, Marriott revised its number to 383 million of potential impacted guest records.

9. Marriott's due diligence during the acquisition process and thereafter failed to reveal that Starwood's guest reservation database and other Starwood systems had been accessed by Hackers from at least July of 2014.

10. On this news, the Company's share price dropped approximately 5.6%, or $6.81, from a closing price of $121.84 per share on November 29, 2018 to close at $115.03 per share on November 30, 2018. Marriott's market capitalization fell more than $2.3 billion in a single day.

11. During the Relevant Period, Defendants breached their fiduciary duties by ignoring red flags (*see* Sections VII.B.(3) and VII.E.), and knowingly or recklessly causing the Company to permit and/or fail to prevent the continuation of the Data Breach.

12. Also, during the Relevant Period, Defendants (defined below) breached their fiduciary duties by personally making and/or causing the Company to make to the investing public a series of materially false and/or misleading statements regarding the Company's business, operations, prospects and legal compliance (see Sections IX and X).

13. Specifically, certain of the Defendants, who served as directors on the Board and/or on the Board's Audit Committee willfully or recklessly made and/or ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and VII.E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of General Data Protection Regulation ("GDPR"). *See* Section VII.D.(4).

14. Defendants also breached their fiduciary duties by failing to correct and/or causing the Company to fail to correct these false and/or misleading statements and/or omissions of material fact to the market.

15. Defendants further breached their fiduciary duties by failing to have Marriott timely notify the impacted Marriott guests of the Data Breach.

16. In addition, during the Relevant Period, Defendants breached their fiduciary duties by causing the Company to repurchase its own stock at prices that were artificially inflated due to the foregoing misrepresentations. Approximately 26 million shares of the Company's common stock were repurchased between October 1, 2017 and September 30, 2018 for over $3.39 billion. As the Company's stock was actually only worth $113.50 per share, the price at which it was

trading when markets closed on December 4, 2018, the Company overpaid over $451.4 million in total.

17. As a result of the Data Breach and Defendants' misconduct, approximately 100 lawsuits have been filed against Marriott and Starwood from a variety of plaintiffs, including residents of all fifty states. On February 6, 2019, various identified lawsuits were transferred to this Court for coordinated or consolidated pretrial proceedings (the "MDL Action"). The MDL Action is organized by the following "Tracks": (1) **The Consumer Track** -- lawsuits against Marriott including claims for violations of the data protection laws of all fifty states; (2) **The Financial Institution Track** -- claims regarding costs to financial institutions stemming from the Data Breach; (3) **The Government Track** -- claims brought by the City of Chicago on behalf of its citizens; (4) **The Securities Track** -- claims brought on behalf of Marriott shareholders for violations of various securities laws (the "Securities Class Action"), and (5) **The Shareholder's Derivative Track** (this action). Each of these Tracks filed consolidated complaints in the MDL Action, some which are referenced herein. The Consumer Track Second Amended Consolidated Complaint (ECF 595-2) is referred to herein as the "Consumer Complaint." The Securities Track Third Amended Consolidated Complaint (ECF 609) is referred to herein as the "Securities Complaint."

18. Further, Marriott is also facing investigations from "certain committees of the U.S. Senate and House of Representatives," and "regulatory authorities in various other jurisdictions [,]" including Attorneys General in various states.

19. As further evidence of Defendants oversight failures and Defendants' failures of maintaining effective internal controls and procedures relating to cybersecurity, on March 31, 2020, Marriott issued a press release disclosing that it had suffered yet another data breach

impacting more than five (5) million of its guests.

## II. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs' claims raise a federal question under Section 14(a) of the Exchange Act, 15 U.S.C. § 78n, Rule 14a-9 of the Exchange Act, 17 C.F.R. § 240.14a-9, Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b), 78t(a) and 78t-1), and SEC Rule 10b-5 (17 C.F.R. § 240.10b-5) promulgated thereunder. This Court has supplemental jurisdiction over the remaining claims under 28 U.S.C. § 1367.

21. This Court has jurisdiction over each defendant named herein because each defendant is either a corporation that conducts business in and maintains operations in this District or is an individual who has sufficient minimum contacts with this District to render the exercise of jurisdiction by the District courts permissible under traditional notions of fair play and substantial justice.

22. Venue is proper in this Court in accordance with 28 U.S.C. § 1391 because: (1) Marriott maintains its principal place of business in this District; (2) one or more of the defendants either resides in or maintains executive offices in this District; (3) a substantial portion of the transactions and wrongs complained of herein, including Defendants' primary participation in the wrongful acts detailed herein, and aiding and abetting and conspiracy in violation of fiduciary duties owed to Marriott, occurred in this District; and (4) Defendants have received substantial compensation in this District by doing business here and engaging in numerous activities that had an effect in this District.

## III. PARTIES

### A. Plaintiffs

23. Plaintiff Moore is, and was at relevant times, a shareholder of Marriott.

24. Plaintiff Alves is, and was at relevant times, a shareholder of Marriott.

**B. Nominal Defendant**

25. ***Nominal Defendant*** Marriott operates, franchises, and licenses hotel, residential, and timeshare properties worldwide. The Company is incorporated in Delaware with locations throughout the world, including New York. Marriott's principal executive offices are at 10400 Fernwood Road, Bethesda, MD 20817.

**C. Director Defendants**

26. ***Defendant Frederick A. Henderson*** ("Henderson") is a director on Marriott's Board, as well as the Chair of the Board's Audit Committee and the Nominating and Corporate Governance Committee. Defendant Henderson has been on Marriott's Board since 2013, the Chair of the Audit Committee since May 2014 and throughout the Relevant Period and began serving on the Nominating and Corporate Governance Committee in 2018. According to Marriott, Defendant Henderson has "significant accounting skills, experience in leading the initial public offering of a subsidiary of a public company, and expertise in large organization management and emerging markets." During the Relevant Period, Defendant Henderson signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

27. ***Defendant Mary K. Bush*** ("Bush") was a director on Marriott's Board from 2008 until May 8, 2020. Defendant Bush also was a member of the Board's Audit Committee and the Board's Compensation Policy Committee. According to Marriott, Defendant Bush has "extensive financial, international and U.S. government experience, her knowledge of corporate governance and financial oversight gained from her membership on the boards of other public companies, knowledge of public policy matters and capital markets and her significant experience in international arenas." During the Relevant Period, Defendant Bush signed SEC filings and made

public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

28. Defendant Bush has attained the age of 72 and therefore was not nominated for re-election as a director, consistent with the retirement policy in the Company's Governance Principles.

29. ***Defendant Aylwin B. Lewis*** ("Lewis") is a director on Marriott's Board, as well as a member of the Board's Audit Committee and the Compensation Policy Committee. Defendant Lewis has been on Marriott's Board since September 2016, having previously been on Starwood's Board of Directors since 2013. Defendant Lewis became a member of the Audit Committee in September 2016 and remained on the Audit Committee through the end of the Relevant Period. According to Marriott, Defendant Lewis has "significant expertise in corporate branding, franchising and management of complex global businesses." During the Relevant Period, Defendant Lewis signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

30. ***Defendant Lawrence W. Kellner*** ("Kellner") is the Lead Director on Marriott's Board, and a member of the Board's Executive Committee and Nominating and Corporate Governance Committee. Defendant Kellner was also a member of the Board's Audit Committee from the beginning of the Relevant Period until September 2016, and a member of the Board's Finance Committee in 2015, 2016, and 2017. Defendant Kellner has been on Marriott's Board since 2002. According to Marriott, Defendant Kellner has experience "with significant management, strategic and operational responsibilities in the travel and leisure industry," as well as "extensive knowledge in the fields of finance and accounting." During the Relevant Period,

Defendant Kellner signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

31. ***Defendant George Muñoz*** ("Muñoz") is a Director on Marriott's Board, as well as a member of the Board's Audit Committee and the Committee for Excellence. Defendant Muñoz was also on the Board's Finance Committee in 2015. Defendant Muñoz has been on Marriott's Board since 2002, became a member of the Audit Committee in September 2016 and remained on the Audit Committee and the Committee for Excellence throughout the Relevant Period. According to Marriott, Defendant Muñoz has "extensive knowledge in the fields of finance and accounting, [] knowledge of international markets, legal experience, corporate governance experience and audit oversight experience gained from his membership on the boards and audit committees of other public companies." During the Relevant Period, Defendant Muñoz signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

32. ***Defendant Arne M. Sorenson*** ("Sorenson") has served on the Marriott Board since 2011. Defendant Sorenson became President and Chief Executive Officer ("CEO") of the Company on March 31, 2012. Prior to that, Defendant Sorenson was President and Chief Operating Officer ("COO") of the Company since May 2009. Defendant Sorenson joined Marriott in 1996 as Senior Vice President of Business Development and was appointed Executive Vice President and CFO in 1998, and assumed the additional title of President, Continental European Lodging, in January 2003. Defendant Sorenson has continuously been a member of Marriott's Executive Committee and Committee for Excellence since at least 2015. Marriott acknowledges and admits that Sorenson is not independent as a result of his employment with the Company.

During the Relevant Period, Defendant Sorenson signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

33. Marriott paid Defendant Sorenson the following compensation as an executive:

| Fiscal Year | Salary | Bonus | Stock Awards | SAR Awards | Non-Equity Incentive Plan Compensation | Value and Nonqualified Deferred Compensation Earnings | All Other Compensation | Total |
|---|---|---|---|---|---|---|---|---|
| 2018 | $1,300,000 | | $6,222,315 | $2,207,473 | $2,925,000 | $23,309 | $255,895 | $12,933,992 |
| 2017 | $1,300,000 | $1,000,000 | $5,310,583 | $1,838,959 | $3,628,950 | $45,635 | $187,490 | $13,311,617 |
| 2016 | $1,236,000 | | $6,010,081 | $2,000,062 | $2,756,527 | $90,184 | $205,524 | $12,298,378 |
| 2015 | $1,236,000 | | $3,830,311 | 2,000,036 | $3,626,919 | $75,740 | $206,411 | $10,975,417 |

34. ***Defendant J.W. Marriott, Jr.*** ("JW Marriott") has served as a director of Marriott since 1964 and has been Chairman of the Board since 1985. Defendant JW Marriott was elected Executive Chairman effective March 31, 2012. Defendant JW Marriott served as CEO of the Company and its predecessors since 1972. Defendant JW Marriott joined Marriott Corporation (formerly Hot Shoppes, Inc.) in 1956, became President in 1964 and CEO in 1972. Defendant JW Marriott relinquished his CEO position in 2012 when he was elected Executive Chairman. Defendant JW Marriott has continuously been the Chair of the Company's Executive Committee since at least 2015. Also, Defendant JW Marriott is the father of Defendant Deborah M. Harrison. In its Schedule 14A ("Proxy Statement") dated April 10, 2019, Marriott acknowledges and admits that Defendant JW Marriott is not independent as a result of his employment with the Company and family relationships.[2] During the Relevant Period, Defendant JW Marriott signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

[2] "Marriott, Jr. [JW Marriott], Deborah M. Harrison, and Arne M. Sorenson are considered not independent as a result of their employment with the Company and/or family relationships." *See* Marriott's Proxy Statement, dated April 10, 2019 at p. 30.

35. Marriott also paid Defendant JW Marriott the following compensation as an executive:

| Fiscal Year | Salary | Change in pension Value and Nonqualified Deferred Compensation Earnings | All Other Compensation | Total |
|---|---|---|---|---|
| 2017 | $3,000,000 | $214,007 | $171,408 | $3,385,415 |
| 2016 | $3,000,000 | $455,752 | $201,864 | $3,657,616 |
| 2015 | $3,000,000 | $434,283 | $194,016 | $3,628,299 |

36. ***Defendant Bruce W. Duncan*** ("Duncan") served on the Marriott Board from 2016 until July 22, 2020. Defendant Duncan was a member of Marriott's Finance Committee in 2016 through 2018 and was a member of Marriott's Audit Committee from 2018 until his departure from Marriott. Before joining Marriott, Defendant Duncan was a Director of Starwood since 1999, served on Starwood's Corporate Governance and Nominating Committee, and was its Chairman of the Board since 2005 and at the time of the merger. During the Relevant Period, Defendant Duncan signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

37. On July 22, 2020, Defendant Duncan resigned from the Board.

38. ***Defendant Deborah M. Harrison*** ("Harrison") has served on the Marriott Board since 2014. Defendant Harrison has been a member of Marriott's Committee for Excellence from at least 2015 to the present and was a member of its Finance Committee from at least 2015 through 2018, when the Finance Committee was dissolved. Defendant Harrison is also the daughter of Defendant JW Marriott. In its Proxy Statement, dated April 10, 2019, Marriott acknowledges and admits that Defendant Harrison is not independent as a result of Harrison's current role as Global Cultural Ambassador Emeritus, and the family relationships of JW Marriott. *See* note 1 above. During the Relevant Period, Defendant Harrison signed SEC filings and made public statements

to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

39. ***Defendant Eric Hippeau*** ("Hippeau") has served on the Marriott Board since 2016. Defendant Hippeau joined Marriott's Compensation Policy Committee on September 23, 2016 and has continuously served on that committee since that date. Before joining Marriott, Defendant Hippeau was a Director of Starwood since 1999, and served on Starwood's Audit Committee and Compensation and Option Committee. During the Relevant Period, Defendant Hippeau signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

40. ***Defendant Debra L. Lee*** ("Lee") has served on the Marriott Board since 2004. Defendant Lee has continuously been the Chairman of Marriott's Committee for Excellence and a member of its Nominating and Corporate Governance Committee since at least 2015. During the Relevant Period, Defendant Lee signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

41. ***Defendant Steven S. Reinemund*** ("Reinemund") served on the Marriott Board from 2007 to May 8, 2020. Defendant Reinemund was the Chairman of Marriott's Compensation Policy Committee and a member of its Nominating and Corporate Governance Committee and Executive Committee since at least 2015. During the Relevant Period, Defendant Reinemund signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

42. Defendant Reinemund has attained the age of 72 and therefore was not nominated for re-election as a director, consistent with the retirement policy in the Company's Governance

Principles.

43. ***Defendant Susan C. Schwab*** ("Schwab") has served on the Marriott Board since 2015. Defendant Schwab has continuously been a member of Marriott's Compensation Policy Committee since at least 2015 and was a member of Marriott's Finance Committee from 2015 through 2018 when the Finance Committee was dissolved. During the Relevant Period, Defendant Schwab signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Sections IX.Q., and Z, and X.A. and B.

44. Defendants Henderson, Bush, Lewis, Kellner and Muñoz are collectively referred to herein as the "Audit Committee Defendants."

45. Defendants Henderson, Bush, Lewis Kellner, Muñoz, Sorenson, JW Marriott, Duncan, Harrison, Hippeau, Lee, Reinemund, Duncan, and Schwab are collectively referred to herein as the "Director Defendants."

**D. Officer Defendants**

46. ***Defendant Bruce Hoffmeister*** ("Hoffmeister") served as Marriott's Chief Information Officer ("CIO") since April 2011 until sometime in 2020. Prior to assuming his current role, Defendant Hoffmeister was a Senior Vice President: IR Shared and Application Services and a Senior Vice President, Global Revenue Management, in addition to holding various other finance and accounting roles within the Development, Information Resources, and Lodging areas. In these roles, Defendant Hoffmeister directed Marriott's process for replacing and updating its Sales and Marketing, Event Management, and Revenue Management systems. During the Relevant Period, Defendant Hoffmeister made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Section IX.Y.

47. ***Defendant Bao Giang Val Bauduin*** ("Bauduin") is Marriott's Global Chief Accounting Officer ("CAO") and Controller. Defendant Bauduin has been in these roles since

June 2014. Prior to becoming CAO of Marriott, Defendant Bauduin was a partner at Deloitte & Touche LLP. Defendant Bauduin has also been Vice President and Manager of Starwood since September 2016. As a part of his role as CAO, Defendant Bauduin is responsible for oversight of Financial Reporting and Analysis, Accounting Policy, Governance, Risk Management, Accenture Hospitality Services, and Corporate Finance Business Partners. During the Relevant Period, Defendant Bauduin signed SEC filings on behalf of Marriott and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Section IX.

48. In addition to his role as CAO, Defendant Bauduin was Marriott's lone signatory for the Company's quarterly reports filed with the SEC on Form 10-Qs and signed each of Marriott's annual reports on Form 10-Ks and current reports on Form 8-Ks during the Relevant Period. *See* Section IX. As such, Defendant Bauduin was not only responsible for reviewing the statements in those filings, but also would have been involved in the process of preparing those filings. In order to carry out those responsibilities, Defendant Bauduin would have to be involved in, or at the very least kept informed of, the due diligence and Integration process related to Starwood. Further, Defendant Bauduin was named a Manager of Starwood at the close of the Merger.

49. ***Defendant Kathleen "Leeny" Kelly Oberg*** ("Oberg") is Marriott's CFO and an Executive Vice President. Defendant Oberg has been in these roles since January 2016. Prior to becoming CFO of Marriott, Defendant Oberg was CFO of the Ritz-Carlton Hotel Company LLC, a Marriott subsidiary. Defendant Oberg started working at Marriott in 1999 and has served in a number of roles with the Company, including Senior VP, Corporate and Development Finance and Senior VP of International Project Finance and Asset Management. Defendant Oberg has also been Manager of Starwood since September 2016, when Marriott acquired Starwood. During the

Relevant Period, Defendant Oberg signed SEC filings and made public statements to the market about Marriott's operations and the Company's acquisition of Starwood. *See* Section IX below.

50. For example, in connection with Marriott's February 12, 2016 meeting of the Board—three months into the Relevant Period, and just seven months before the Merger closed—Defendant Oberg distributed a slide presentation to the Board, including the Audit Committee Defendants and Defendant Sorenson. The presentation included a slide titled "Overall Company Risk Ranking" that ranked the top risks facing Marriott in 2016. One slide showed that the Board itself ranked cybersecurity as the number one risk facing Marriott in 2016. Another slide presented to Defendant Sorenson and the Director Defendants, including the Audit Committee Defendants, stated that "the Board of Directors and Management both view [cybersecurity] risk as having increased from 2015 to 2016" and "[c]ybersecurity is an enterprise-wide risk that continues to make headlines and present challenges for many large organizations due to the sophistication of cyber events and the related costs . . . . Large-scale cybersecurity breaches can quickly erode customer confidence and result in significant brand damage."

51. Defendant Oberg presented to the Board (the Director Defendants), which included Defendant Sorenson and the Audit Committee Defendants, on cybersecurity risk at least three (3) times during the Relevant Period. Defendant Oberg reminded the Board regularly that cybersecurity was a priority for Marriott, and that Marriott needed to mitigate cybersecurity related risks, and specifically maintained that "continuous efforts to identify and mitigate risks [are] required." *See* Sections IV.(3) and (4), and VII,G.

52. Defendant Oberg was also named Manager of Starwood upon the closing of the Merger. As Manager of the newly acquired entity, Defendant Oberg would have been intricately involved in the Integration process. Additionally, as CFO Defendant Oberg would be informed

regarding the decision to perform information security due diligence as well as responsible for reporting the result to the Board (the Director Defendants). Given her involvement in both the Merger and Integration process, Defendant Oberg knew or was severely reckless in not knowing that the public statements to the market issued by the Company omitted material information throughout the Relevant Period which would have made the statements regarding Marriott's due diligence, data security and cybersecurity policies and practices, and cybersecurity risks false and misleading when made. Defendant Oberg was at least severely reckless in failing to disclose this information.

53. Additionally, as a member of Marriott's senior management, and a regular presenter on cybersecurity risk at Marriott's Board meetings throughout the Relevant Period, Defendant Oberg was aware of the cybersecurity and data security risks and red flags Marriott faced. Despite knowledge of these risks and red flags, throughout the Relevant Period, Defendant Oberg signed Sarbanes-Oxley Act ("SOX") Certifications indicating that she had reviewed each of the Form 10-Ks and Form 10-Qs Marriott filed throughout the Relevant Period, and that those filings did not contain any material false and misleading statements.

54. Marriott paid Defendant Oberg the following compensation as an executive

| Fiscal Year | Salary | Bonus | Stock Awards | SAR Awards | Non-Equity Incentive Plan Compensation | Change in Pension Value and Nonqualified Deferred Compensation Earnings | All Other Compensation | Total |
|---|---|---|---|---|---|---|---|---|
| 2018 | $772,500 | | $1,940,374 | $883,017 | $996,526 | $4,683 | $107,957 | $4,705,057 |
| 2017 | $750,000 | $500,000 | $1,713,792 | $765,020 | $1,046,850 | $7,141 | $77,167 | $4,859,970 |
| 2016 | $650,000 | | $2,977,048 | $600,045 | $724,815 | $11,086 | $37,237 | $5,000,951 |

55. Defendants Sorenson, Hoffmeister, Bauduin, and Oberg are referred to herein as the "Officer Defendants."

56. The Director Defendants and Officer Defendants are collectively referred to herein

as the "Defendants."

## IV. MARRIOTT'S CORPORATE GOVERNANCE

57. As members of Marriott's Board, the Director Defendants were held to the highest standards of honesty and integrity and charged with overseeing the Company's business practices and policies and assuring the integrity of its financial and business records.

58. The conduct of the Director Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and officers of Marriott, the absence of good faith on their part, and a reckless disregard for their duties to the Company and its investors that the Director Defendants were aware posed a risk of serious injury to the Company.

59. As stated in Marriott's Proxy Statement, dated April 4, 2018, its Board has six standing committees: Audit; Compensation Policy; Finance; Nominating and Corporate Governance; Committee for Excellence (now known as the Inclusion and Social Impact Committee); and Executive. As stated in its Proxy Statement, dated April 10, 2019, the Finance Committee was dissolved in November 2018 upon the Board's determination that it had completed its assigned tasks.

### A. Business Conduct Guide

60. Marriott maintains a Business Conduct Guide (the "Code of Ethics") which is available to the investing public on its website. It begins with a quote from Defendant JW Marriott stating "***Our business relies on integrity and good judgment***." (Emphasis added). This Business Conduct Guide further states in relevant part:

> **What is Expected of Everyone?**
>
> As Marriott associates, officers, directors, or other persons acting on behalf of Marriott (collectively "associates"), you are expected to be familiar with and work within the code of business conduct detailed in this Business Conduct Guide.
>
> * * *

**Who is Responsible?**

All Marriott associates are responsible for upholding the legal, ethical, and social standards detailed in the Business Conduct Guide.

* * *

**Customer and Associate Privacy**

There are strict policies concerning the disclosure of information about Marriott guests and associates.

There are only limited circumstances in which private information of associates or customers may be disclosed outside of Marriott.

You are responsible for reviewing and understanding Marriott policies before you release information about Marriott customers and associates. Other than the exceptions expressly identified in Marriott policies, you may not disclose records and information concerning present or former customers or associates.

This private information includes any Personally Identifiable Information (PII), which can be associated with or traced to an individual, such as:

> *Name, address, telephone number, e-mail address, government issued identifications (e.g., Social Security Number), health records, credit card information, or other financial information.*

***Information concerning customers and associates must be safeguarded*** and should be used only for legitimate business purposes and should not be shared, even with Marriott, except on a need-to-know basis. [Emphasis added]

**More Information**:

Consult **MIP-47 ("Personal Information Privacy")** for more information regarding PII

61. Although Marriott refers to its MIP-47 (regarding Personal Information Privacy) in its Business Conduct Guide, this document does not appear on Marriott's website using that title or reference number and is not otherwise available to the investing public.

62. Regarding "Accurate Books, Records, and Reports," the Code of Ethics provides, in relevant part, that:

> Be honest and act with integrity in all communications … in every record created and in all data entered, from financial information and personal resumés to quality and safety reports. Our books, records, and reports are only as accurate as the data from which they are derived.
>
> * * *
>
> Make certain that all information and reports supplied to government authorities, self-regulatory organizations (such as the Financial Industry Regulatory Authority), shareholders, securities analysts, and the general public are accurate, timely, and supported by necessary documentation.

63. With respect to "Dealing Fairly With Customers," the Code of Ethics provides that:

> As a leading worldwide hospitality company, Marriott is dedicated to providing exceptional customer service. Customers should always be treated fairly and with respect.
>
> Customers should be given what is promised and at the promised price. Misrepresentations about Marriott's products and services may lead to costly legal action. A false claim, a small untruth, or even a perception of dishonesty can jeopardize the loyalty and satisfaction of our customers.
>
> When communicating with customers and the public:
>
> - Be truthful, without embellishment or omission, when representing the nature and quality of Marriott's products, services, prices, contractual terms, and other information.
>
> - Avoid even inadvertently misleading customers.
>
> - Only make claims about Marriott's products and services that you know to be true or have adequate information to support.

64. The Code of Ethics provides, as to "fair and ethical dealing," that:

> Every employee must promote positive business relationships. ***Never gain unfair advantage by misleading, misrepresenting or deceiving***.
>
> ***We do not participate in false or deceptive advertising of our products, services or our Company***. Make sure that you are truthful and accurate in promotional materials, including advertising, sales, and marketing communications; and, ensure that you can substantiate any claims that you make. [Emphasis added]

65. The Code of Ethics provides, regarding "Providing Information to the

Government" in relevant part, that:

> Always be truthful in providing information to the government on behalf of Marriott.
>
> You may interact with various government agencies in many ways.
>
> Examples include:
>
> - Filing routine information with government agencies (e.g., tax returns, lobbying disclosure reports, securities filings)
> - Participating in legal actions before agencies and courts
> - Participating in legal actions before agencies and courts
>
> Making false statements in these circum-stances [sic] may harm Marriott's reputation and may result in severe penalties for both Marriott and the responsible associate.
>
> Never attempt to obstruct a government inquiry or the administration of justice, and immediately report any such activities by others.

66. The Code of Ethics provides, as to "Protecting Confidential Information," that:

> Everyone is responsible for protecting the confidentiality of Marriott's proprietary information, except when disclosure is authorized or legally mandated.
>
> This duty applies to all associates. It applies during both working and nonworking hours and extends beyond your employment with Marriott.
>
> Do not share Marriott's confidential information with: 1) associates who are not authorized to receive it or do not have a business need for the information; or 2) persons outside Marriott, unless there is a legitimate and authorized business purpose for the disclosure, or unless disclosure is required by law.
>
> **Confidential Information Includes:**
>
> • Information that derives value from not being known to the public
>
> • Undisclosed or commercially sensitive information that might be of use to Marriott's competitors
>
> • Information that might harm Marriott, our shareholders, our customers, or our associates, if disclosed
>
> **Examples of Confidential Information:**

• ***Personal and financial information concerning customers or associates***

* * *

**Defer to Designated Persons**

To protect Marriott and our shareholders and to ensure compliance with the law, decisions related to disclosing commercially sensitive business information and other nonpublic information should be made only by designated persons and coordinated with the Communications Department.

Never share information about Marriott with the news media, government officials, shareholders, securities analysts, other interested persons, or the public, without proper authorization or as required by law. [Bold subheadings in original, bold & italic emphasis added.]

67. Regarding "Protecting Marriott's Reputation," the Code of Ethics provides, in relevant part: "***You must avoid any communication, disclosure, or interaction that might*** disparage, defame, or ***damage Marriott's reputation***, associates, customers, vendors, or other business partners, or that might fail to serve the best interests of our shareholders. [Emphasis added].

68. Regarding "Customer and Associate Privacy," the Code of Ethics provides, in relevant part:

There are strict policies concerning the disclosure of information about Marriott guests and associates.

There are only limited circumstances in which the private information of associates or customers may be disclosed outside of Marriott.

You are responsible for reviewing and understanding Marriott policies before you release information about Marriott customers and associates. Other than the exceptions expressly identified in Marriott policies, you may not disclose records and information concerning present or former customers or associates.

***This private information includes any Personally Identifiable Information (PII), which can be associated with or traced to an individual***, such as:

*Name, address, telephone number, e-mail address, government issued identifications (e.g., Social Security number), health records, credit card information, or other financial information*

> ***Information concerning customers and associates must be safeguarded and should be used only for legitimate business purposes and should not be shared***, even within Marriott, except on a need-to-know basis. [Italicized text in original. Emphasis added in bold & italics.]

69. In violation of the Code of Ethics, the Director Defendants conducted little, if any, oversight of the Company's engagement in Defendants' scheme to issue materially false and misleading statements to the public and to facilitate and disguise Defendants' violations of law, including breaches of fiduciary duty, waste of corporate assets, unjust enrichment, and violations of Sections 14(a), 10(b), and 20(a) of the Exchange Act. Moreover, in violation of the Code of Ethics, Defendants failed to maintain the accuracy of Company records and reports, comply with laws and regulations, protect customer information and the Company's reputation, or conduct business in an honest and ethical manner.

**B. Governance Principles**

70. Marriott's Governance Principles (Revised May 6, 2016[3]) states in relevant part:

> **Director Qualifications**. The board's Nominating and Corporate Governance Committee selects director candidates based on character, judgment, business and professional experience and reputation, personal and professional ethics, integrity, values and familiarity with national and international issues affecting business. Board members are selected who not only bring a depth of experience but also provide skills and knowledge complementary to the board and Marriott's business. Candidates must be committed to representing the long-term interests of the shareholders.
>
> * * *
>
> **Ethics and Conflicts of Interest**. The board expects Marriott's directors, officers and employees to act ethically at all times and acknowledge their adherence to Marriott's Code of Ethics, and Marriott's officers and directors to follow Marriott's Business Conduct Guide….
>
> * * *
>
> **Access to Independent Advisors**. The board and its committees have the responsibility at any time to retain independent outside financial, legal or other

[3] Marriott's Governance Principles were revised again in November 2019.

advisors if at any time such advice is required to fulfill their obligations

**Director Orientation**. The general counsel and the chief financial officer provide an orientation for new directors, and periodically provide materials or briefing sessions for all directors on subjects that would assist them in discharging their duties….

**C. Audit Committee Charter**

71. Marriott has an Amended and Restated Audit Committee Charter (as of August 6, 2015), which outlines the responsibilities of the Audit Committee. The Audit Committee's responsibilities include risk assessment, and the Audit Committee Charter states, in relevant part:

Purpose; Statement of Policy

The purpose of the Audit Committee (the "Committee") is to represent and assist the Board of Directors in overseeing: (i) the accounting, reporting, and financial practices of the Company and its subsidiaries, including the integrity of the Company's financial statements; (ii) ***the Company's internal control environment and compliance with legal and regulatory requirements***; (iii) the independent auditors' qualifications and independence; and (iv) the performance of the Company's internal audit function and the independent auditor.

* * *

Duties and Responsibilities

Consistent with and subject to applicable law and rules or listing standards promulgated by the SEC, NASDAQ, or other applicable regulatory authority, the Committee shall have the following duties and responsibilities.

* * *

*Risk Assessment and Control Environment*

The Committee will periodically review and discuss the Company's business and financial risk management and risk assessment policies and procedures with senior management, the Independent Auditor, and the Chief Audit Executive.

*Internal Controls and Disclosure Controls and Procedures*

The Committee will periodically review and discuss with the internal auditors and the Principal Independent Auditor the adequacy and effectiveness of the Company's internal control environment, including any

significant deficiencies or material weaknesses and any significant changes in internal controls that are required to be disclosed in the Company's periodic filings. The Committee will also review the annual report of the Principal Independent Auditor on the Company's internal controls over financial reporting. In connection with this review, the Committee will obtain and discuss:

1. Reports from the Chief Executive Officer, the Chief Financial Officer, and the Principal Independent Auditor on any significant deficiencies in the design or operation of internal controls with the identification of any material weakness;

2. Any fraud or other irregularity (whether or not material) that involves management or other employees who have a significant role in the Company's internal control environment; and

3. Management's evaluations of the Company's internal controls over financial reporting and disclosure controls and procedures.

* * *

*Compliance*

The Committee will oversee the Company's compliance systems with respect to legal and regulatory requirements and review the Company's compliance policies and its programs to monitor compliance with these policies. In this regard, the Committee will:

1. At least annually review with management, the General Counsel, and the Chief Audit Executive the Company's programs to promote compliance with its Ethical Conduct Policy (MIP-1) and the Business Conduct Guide. These policies will be posted on the Company's public website; and

2. Establish and oversee a procedure for the oversight and reporting to the Committee of the receipt, retention, treatment, and closure of complaints to the Company concerning (i) accounting, internal accounting controls, or auditing matters; or (ii) the confidential, anonymous submission by Company employees regarding questionable accounting or auditing matters.

3. Review findings of regulatory agencies' examination.

*Information Protection and Privacy*

> The Committee will review and discuss with management at least semiannually the Company's privacy and data security risk exposures, including: 1. The potential impact of those exposures on the Company's business, financial results, operations and reputation;
>
> 1. The potential impact of those exposures on the Company's business, financial results, operations and reputation;
>
> 2. The steps management has taken to monitor and mitigate such exposures;
>
> 3. The Company's information governance policies and programs; and
>
> 4. Major legislative and regulatory developments that could materially impact the Company's privacy and data security risk exposure.
>
> * * *
>
> *Investigations*
>
> The Committee may investigate suspected improprieties on any material matter, using special counsel or outside experts when necessary or appropriate.

72. In violation of their duties as members of the Audit Committee, the Audit Committee members failed to effectively review and discuss risks associated with cybersecurity and failed to effectively review and discuss with the independent auditor the adequacy and effectiveness of the Company's internal controls.

**D. Nominating and Corporate Governance Charter**

73. Marriott's Amended and Restated Nominating and Corporate Governance Committee Charter (Revised August 6, 2015) states in relevant part:

> **Duties and Responsibilities**
>
> The Committee's duties and responsibilities shall be as follows:
>
> * * *
>
> To review and, as appropriate, make recommendations regarding the effective functioning of the Board such as the quality, quantity and timeliness

> of information furnished to Directors and frequency and location of Board meetings.
>
> * * *
>
> The Committee shall develop and recommend to the Board for its approval a set of corporate governance principles. The Committee shall review the principles on at least an annual basis and recommend changes as necessary[4].

## V. DUTIES OF DEFENDANTS

74. By reason of their positions as officers and/or directors of the Company, and because of their ability to control the business and corporate affairs of Marriott, Defendants owed Marriott and its investors the fiduciary obligations of trust, loyalty, and good faith. The obligations required Defendants to use their utmost abilities to control and manage Marriott in an honest and lawful manner. Defendants were and are required to act in furtherance of the best interests of Marriott and its investors.

75. Each director and officer of the Company owes to Marriott and its investors the fiduciary duty to exercise loyalty, good faith, and diligence in the administration of the affairs of the Company and in the use and preservation of its property and assets. The conduct of Defendants complained of herein involves a knowing and culpable violation of their obligations as directors and officers of Marriott, the absence of good faith on their part, or a reckless disregard for their duties to the Company and its shareholders that Defendants were aware or should have been aware posed a risk of serious injury to the Company. The conduct of Defendants who were also officers and directors of the Company has been ratified by the remaining Defendants who collectively comprised Marriott's Board at all relevant times

76. In addition, as senior executive officers and directors of a publicly-traded company

[4] Marriott's Audit Committee Charter and Nominating and Corporate Governance Charter were revised again in November 2019.

whose common stock was registered with the SEC pursuant to the Exchange Act and traded on the NASDAQ, Defendants had a duty to prevent and not to effect the dissemination of inaccurate and untruthful information with respect to the Company's financial condition, performance, growth, operations, financial statements, business, products, management, earnings, internal controls, cybersecurity risks, and present and future business prospects, and had a duty to cause the Company to disclose omissions of material fact in its regulatory filings with the SEC all those facts described in this Complaint that it failed to disclose, so that the market price of the Company's common stock would be based upon truthful and accurate information. Additionally, Defendants had a duty not to cause the Company to waste corporate assets by making the Company repurchase its own stock at artificially inflated prices, to the detriment of the Company and its shareholders.

77. To discharge their duties, the officers and directors of Marriott were required to exercise reasonable and prudent supervision over the management, policies, practices, and controls of the affairs of the Company. By virtue of such duties, the officers and directors of Marriott were required to, among other things:

(a) ensure that the Company complied with its legal obligations and requirements, including acting only within the scope of its legal authority and disseminating truthful and accurate statements to the SEC and the investing public;

(b) conduct the affairs of the Company in an efficient, businesslike manner so as to make it possible to provide the highest quality performance of its business, to avoid wasting the Company's assets, and to maximize the value of the Company's stock;

(c) properly and accurately guide investors and analysts as to the true financial condition of the Company at any given time, including making accurate statements about the Company's business prospects, and ensuring that the Company maintained an adequate

system of financial controls such that the Company's financial reporting would be true and accurate at all times;

(d) remain informed as to how Marriott conducted its operations, and, upon receipt of notice or information of imprudent or unsound conditions or practices, make reasonable inquiries in connection therewith, take steps to correct such conditions or practices, and make such disclosures as necessary to comply with federal and state securities laws;

(e) ensure that the Company was operated in a diligent, honest, and prudent manner in compliance with all applicable federal, state and local laws, and rules and regulations; and

(f) ensure that all decisions were the product of independent business judgment and not the result of outside influences or entrenchment motives.

78. At all times relevant hereto, Defendants were the agents of each other and of Marriott and were at all times acting within the course and scope of such agency.

79. Because of their advisory, executive, managerial, and directorial positions with Marriott, each of Defendants had access to adverse, non-public information about the Company.

80. Defendants, because of their positions of control and authority, were able to and did, directly or indirectly, exercise control over the wrongful acts complained of herein, as well as the contents of the various public statements issued by Marriott.

81. Each Defendant, by virtue of his position as a director and/or officer, owed to the Company and to its shareholders the fiduciary duties of loyalty, good faith, and the exercise of due care and diligence in the management and administration of the affairs of the Company, as well as in the use and preservation of its property and assets. The conduct of Defendants complained of

herein involves a knowing and culpable violation of their obligations as directors and officers of Marriott, the absence of good faith on their part, and a reckless disregard for their duties to the Company and its shareholders that Defendants were aware, or should have been aware, posed a risk of serious injury to the Company.

82. Defendants breached their duties of loyalty and good faith by causing the Company, among other things, to issue false and misleading statements concerning the business results and prospects of the Company. As a result, Marriott has expended, and will continue to expend, significant sums of money related to investigations and lawsuits.

## VI. CONSPIRACY, AIDING AND ABETTING, AND CONCERTED ACTION

83. In committing the wrongful acts alleged herein, Defendants have pursued, or joined in the pursuit of, a common course of conduct, and have acted in concert with and conspired with one another in furtherance of their wrongdoing. Defendants caused the Company to conceal the true facts as alleged herein. Defendants further aided and abetted and/or assisted each other in breaching their respective duties.

84. The purpose and effect of the conspiracy, common enterprise, and/or common course of conduct was, among other things, to: (i) facilitate and disguise Defendants' violations of law, including breaches of fiduciary duty, unjust enrichment, waste of corporate assets, and violations of Sections 14(a), 10(b), and 20(a) of the Exchange Act; (ii) conceal adverse information concerning the Company's operations, financial condition, legal compliance, future business prospects and internal controls; and (iii) to artificially inflate the Company's stock price while the Company repurchased its own stock.

85. Defendants accomplished their conspiracy, common enterprise, and/or common course of conduct by causing the Company purposefully, recklessly, or negligently to conceal

material facts, fail to correct such misrepresentations, and violate applicable laws. In furtherance of this plan, conspiracy, and course of conduct, Defendants collectively and individually took the actions set forth herein. Because the actions described herein occurred under the authority of the Board, each of Defendants who are, or were at relevant times, directors of Marriott, was a direct, necessary, and substantial participant in the conspiracy, common enterprise, and/or common course of conduct complained of herein.

86. Each Defendant aided and abetted and rendered substantial assistance in the wrongs complained of herein. In taking such actions to substantially assist the commission of the wrongdoing complained of herein, each Defendant acted with actual or constructive knowledge of the primary wrongdoing, either took direct part in, or substantially assisted the accomplishment of that wrongdoing, and was or should have been aware of his or her overall contribution to and furtherance of the wrongdoing.

87. At all times relevant hereto, each Defendant was the agent of each of the other Defendants and of Marriott and was at all times acting within the course and scope of such agency.

## VII. SUBSTANTIVE ALLEGATIONS

### A. Starwood Background

88. Starwood was originally formed in 1991 by Starwood Capital Partners, a Chicago-based real estate investment firm founded by Barry Sternlicht.

89. In 1999, Starwood started its guest loyalty program known as the Starwood Preferred Guest Program ("SPG Program"). The SPG Program was intended to create brand loyalty and encourage travelers to stay at its properties by offering rewards. Starwood promoted the SPG Program stating, "The program makes headlines with its policy of no blackout dates, no

capacity controls, and online redemption – all industry firsts."[5]

90. Like Marriott, Starwood collected, collects and stores significant amounts of sensitive customer information. By way of example, Starwood's October 15, 2014 online privacy statement stated that Starwood is "dedicated to protecting your privacy and safeguarding your personally identifiable information" and "collects information about our guests and visitors to our web sites so that we can provide an experience that is responsive to our guests' and visitors' needs." The statement also stated in relevant part:

> **TYPES OF INFORMATION WE COLLECT:**
>
> Starwood collects information about our guests and visitors to our web sites so that we can provide an experience that is responsive to our guests' and visitors' needs. Information may be collected as part of: (i) fulfilling reservation or information requests, (ii) purchasing products or services, (iii) registering for program membership, (iv) submitting a job application, (v) responding to communications from us (e.g., surveys, promotional offers, or reservation confirmations), (vi) accommodating your personal preferences, (vii) fulfilling requests for services or recommendations we provide you, (viii) working with third party sources, including collecting information available from social networking and other web sites, to better assist us with understanding your interests and to serve you better, (ix) your use of our apps on your electronic devices, (x) updating your contact information including your address (through such services as the National Change of Address Service in the United States), or (xi) facilitating the transmission of forward to a friend email at your request. The types of personally identifiable information (sometimes referred to as "PII") that we collect may include your name, home, work and e-mail addresses, telephone, mobile telephone, and fax numbers, credit card information, date of birth, gender, and lifestyle information such as room preferences, leisure activities, names and ages of children, and other information necessary to fulfill special requests (e.g., health conditions that require special room accommodations).
>
> Starwood may also collect non-personally identifiable information about you, such as your use of our web sites, communication preferences, travel habits, aggregated data relative to your stays, and responses to promotional offers and surveys.
>
> ***
>
> PURPOSE FOR COLLECTION, PROCESSING, AND DISCLOSURE:

[5] *See* Starwood Corporate Overview at https://marriott.gcs-web.com/static-files/4cb4e011-ddff-4613-984f-1e08d799227c (Last visited Aug. 4, 2020).

**Collection & Use**

Starwood is fully committed to providing you with information about the collection and use of PII furnished by, or collected from, visitors while using our web sites, products and services. It is our practice not to ask you for information unless we need it or intend to use it. Some of the primary purposes for collecting your PII are as follows:

- providing services such as processing a transaction (e.g., making a reservation, fulfilling a request for information, or completing a product order)
- marketing and communications with you in relation to the products and services offered by Starwood, our strategic marketing partners, and other trusted third parties
- performing market research via surveys to better serve your needs, improve the effectiveness of our web sites, your hotel experience, our various types of communications, advertising campaigns, and/or promotional activities

***

**Processing and Disclosure**

In most cases, the information you provide is added to a local or global database. In the course of processing your information, it may be necessary to transfer your PII to Starwood's affiliates, properties within the Starwood system and/or third party service providers located in the United States and throughout the world for the purposes outlined within this Privacy Statement. Unless otherwise precluded or governed by legal requirements and/or process, Starwood subsidiaries, affiliates and property owners that may receive your information are required to abide by substantially similar privacy requirements relating to your PII. As a general practice, Starwood does not sell, rent, or give physical possession of your PII to unaffiliated third parties outside the Starwood system. Situations in which Starwood may disclose your information to others include:

- when we have received your consent to do so
- in situations where sharing or disclosing your information is required in order to offer you products or services you desire (e.g., a vacation package)
- when companies or services providers that perform business activities on behalf of Starwood require such information (e.g., credit card processing, customer support services, market research administration or database management services)
- when a hotel or other property leaves the Starwood system and access to your PII is necessary to facilitate business operations or meet contractual obligations in connection with the fulfillment of reservations that are booked for future stays or events
- in the event Starwood is merged or acquired by another company

- to comply with legal or regulatory requirements or obligations in accordance with applicable law, a court order or a subpoena
- in case of emergency such as to safeguard the life, health, or property of an individual

If information is shared as mentioned above, we seek to limit the scope of information that is furnished to the amount necessary for the performance of the specific function. Unless otherwise precluded by legal process, we require third parties to protect your PII and abide by applicable privacy laws and regulations.

***

DATA TRANSFERS ACROSS INTERNATIONAL BORDERS:

As a global company, we endeavor to provide you with the same outstanding service in New York City, as you would find in Paris or Beijing. To achieve this goal, we have established a global network comprised of properties, offices, data centers, trusted marketing partners, service providers, customer contact centers, and trained associates around the globe. The nature of our business and our operations require us to transfer your information, including PII, to other group companies, properties, centers of operations, data centers, or service providers that may be located in countries outside of your own. We may transfer the PII we collect about you to countries other than the country in which the information was originally collected. Although the data protection and other laws of these various countries may not be as comprehensive as those in your own country, Starwood will take appropriate steps to ensure that your PII is protected and handled as described in this Privacy Statement.

***

SECURITY SAFEGUARDS:

Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your PII against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls" and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.

91. As reported by *crn.com* in a March 15, 2010 article titled "Accenture Books $200

Million Deal With Starwood", it was revealed that in 2009, Accenture and Starwood entered into a $200 million contract to outsource the maintenance of Starwood's information technology ("IT") and security infrastructure to Accenture. Accenture's services included "development, testing, maintenance and running of the applications. Infrastructure outsourcing services include server and storage management, data center management, end-user computing, network management and service desk management."

92. Notably, as early as November 2015, during the Company's announced merger plans with Starwood, Starwood's IT systems contained significant vulnerabilities due to an outdated version of the Oracle application portal that involved more than 150 applications—including Starwood's reservation of SPG Loyalty Points systems. The archaic system had not been maintained or updated to protect and prevent against hacking. In fact, the Oracle application portal system was substantially outdated (by at least seven years), without maintenance, leaving Starwood significantly vulnerable to attacks from cyber hackers. Starwood's Oracle system had been neglected for so long that repair was no longer a possibility. The system itself had to be upended, which would have costed the company hundreds of millions of dollars to address. The Oracle application remained dangerously unsecured throughout the Company's purported due diligence efforts as further discussed herein—the bare minimum of which would have easily detected such a clear hazard. As such, numerous applications were wide open and susceptible to attack.

93. As discussed herein, at or around this same time (i.e., on November 20, 2015) Starwood publicly disclosed that more than 50 of its hotels had been infected by a malware attack designed to help cyber thieves steal credit and debit card data (the "2015 Starwood Data Breach"). A December 3, 2018 *Forbes* article entitled, "Revealed: Marriott's 500 Million Hack Came After

A String Of Security Breaches" discusses (in addition to the 2015 Starwood Data Breach)other examples of corruption of the Starwood IT systems including (1) that at least six servers hosting various starwoodhotels.com domains were controlled by Russian botnets, which was "… stealing tens of gigabytes from victim systems including vital files and taking screenshots", (2) use of an easily guessable password for Starwood's ServiceNow cloud computing service, creating the opportunity to access businesses' financial records, IT security controls and bookings information (3) going back to 2014, Starwood had a vulnerability on the company's website, which was infected with an SQL injection bug, and (4) vulnerabilities in Starwood's system were being advertised on the dark web.

94. As alleged herein, Starwood failed to implement and maintain reasonable safeguards that resulted in the exposure and exfiltration of the Personal Information for hundreds of millions of hotel guests notwithstanding its representation that it "recognized the importance of keeping its valuable customer information secure" and had "security measures in place to help protect" consumers against "unauthorized access" of their Personal Information.

**B. Marriott Background**

95. Marriott is a worldwide operator, franchisor, and licensor of hotel, residential, and timeshare properties under numerous brand names at different price and service points. It was organized as a corporation in Delaware in 1997 and became a public company in 1998 when it was "spun off" as a separate entity by the company formerly named "Marriott International, Inc."

96. Marriott's guest reservation database and customer data (more fully described below) are important parts of Marriott's core operations. Marriott relies on guest data to bring guests to the Company's hotels and needs its reservation systems to logistically book and obtain payment information for the rooms. Once those guests are in the hotel, Marriott continues to earn

revenues and relating to those systems. As a hotel business, there is no part of Marriott's operations that was not affected by, or connected to, customer reservations and the data those customers provide.

97. Defendants Sorenson and Oberg, among other Marriott executives, repeatedly made public statements about the importance of customer data to the Merger and Marriott's operations generally. These public statements serve as further evidence that Marriott's guest reservation database and customer data are important parts of its core operations.

**(1) Data Collected by Marriott**

98. During the Relevant Period, Marriott collected and continues to collect customer data in the form of credit card numbers, expiration dates and other relevant credit card information ("payment card data" or "PCD") and other personal information ("personally identifiable information" or "PII") from its customers (also described as "guests" by Marriott and herein). This information was and is collected by Marriott (and stored in its guest reservation database) when customers reserve rooms and/or check in at one of Marriott's properties, and possibly at other times. As articulated in the Privacy Policy posted on the Company's website, the Company collects the following PII:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference

- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data
- Prior guest stays or interactions, goods and services purchased, special service and amenity requests
- Geolocation information
- Social media account ID, profile photo and other data publicly available, or data made available by linking your social media and loyalty accounts

99. The Privacy Policy continues, clarifying that the Company also collects:

- Data about family members and companions, such as names and ages of children
- Biometric data, such as digital images
- Images and video and audio data via: (a) security cameras located in public areas, such as hallways and lobbies, in our properties; and (b) body-worn cameras carried by our loss prevention officers and other security personnel
- Guest preferences and personalized data ("**Personal Preferences**")[6] such as your interests, activities, hobbies, food and beverage choices, services and amenities of which you advise us or which we learn about during your visit.

100. The Privacy Policy further assures customers that "[w]e seek to use reasonable organizational, technical and administrative measures to protect Personal Data."

101. Defendants are well aware of the value of PII and PCD. By way of example, Marriott employs a customer analytics company for the systematic examination of its customer information to identify, attract, and retain the most profitable customers and to predict future

[6] Emphasis in original unless otherwise noted throughout.

behaviors. Eric Jacobs, the chief development officer for Marriott International – U.S. and Canada stated, "there is no lack of available data: household profile, including number of kids; type of jobs held by family members; their salaries; where and how they spend their money and even the type of jeans they buy."[7]

**(2) Marriott's Disclosures Regarding Technology, Information Protection and Privacy Risks**

102. At all relevant times, Defendants knew (or were reckless in disregarding) the risks associated with its collection, use, and storage of its customers PCD and PII. In fact, Marriott's Form 10-K for the fiscal year ended December 31, 2017 and filed with the SEC on February 15, 2018 (the "2017 Form 10-K") discusses risks associated with its handling of this information under the section "Risks Relating to Our Business" which states in relevant part:

> Technology, Information Protection, and Privacy Risks
>
> * * *
>
> *We are exposed to risks and costs associated with protecting the integrity and security of company employee and guest data*. ***Our businesses process, use, and transmit large volumes of employee and guest data, including credit card numbers and other personal information*** in various information systems that we maintain and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that guest, employee, and company data is critical to our business***. If that data is inaccurate or incomplete, we could make faulty decisions.
>
> ***Our guests and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information***. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able

[7] *See* Hotelmanagement.net 1/31/18 article, "Marriott bets on predictive analytics for brand growth" at https://www.hotelmanagement.net/tech/marriott-builds-its-brands-by-knowing-more-about-you. (Last visited Aug. 4, 2020).

> to satisfy these changing legal and regulatory requirements and employee and guest expectations, or may require significant additional investments or time to do so.
>
> *Cyber-attacks could have a disruptive effect on our business*. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation***. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits. In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all. [Emphasis added]

103. Marriott's Form 10-K's for the fiscal years ended December 31, 2016 and December 31, 2015 contain substantially similar language regarding Technology, Information Protection, and Privacy Risks when compared to 2017 Form 10-K. This language contained in Marriott's Form 10-Ks and other public filings gave (and gives) the false impression to the investing public that the systems storing Marriott and Starwood customer data (including PII and PCD) were secure.

104. At all relevant times and in a further effort to assure its customers and the investing public, Marriott maintained and published its Global Privacy Statement on its website, which it updated from time to time. Each statement lists the type of personal information it collects from its guests, which list includes PII and PCD data. Regarding Security of Personal Information, Marriott's various Global Privacy Statements state:

(a) From May 21, 2015 - June 30, 2016: "We treat the personal information you provide to us as confidential and take reasonable steps, including standard industry safeguards to protection your personal information from accidental deletion or loss and unauthorized access, disclosure or modification. When you submit personal information to us via our Websites, it is transferred over a Secured Sockets Layer (SSL) connection, provided you are using a SSL enabled browser or device."

(b) From July 1, 2016 - May 17, 2018: "We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section below."

(c) From May 18, 2018 - February 3, 2019: "We seek to use reasonable organizational, technical and administrative measures to protect Personal Data. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below."

- This version of the Global Privacy Statements adds for the first time a "Sensitive Data" section which states, "Unless specifically requested, we ask that you not send us, and you not disclose, on or through the Services or otherwise to us, any Sensitive Personal Data (*e.g.*, social security numbers, national identification number,

data related to racial or ethnic origin, political opinions, religion, ideological or other beliefs, health, biometrics or genetic characteristics, criminal background, trade union membership, or administrative or criminal proceedings and sanctions)."

(d) From February 4, 2019 – Present: "We seek to use reasonable organizational, technical and administrative measures to protect Personal Data. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below."

- This version of the Global Privacy Statements includes a "Sensitive Data" section with the same language as quoted above.

**(3) What Defendants Knew and When They Knew It**

105. In an August 7, 2014 Board meeting attended by Defendants JW Marriott, Bush, Harrison, Henderson, Kellner, Lee, Muñoz, Reinemund, Sorenson, and others, they discussed "some recent publicized [data breach] incidents," including the Target data breach. These Defendants also received a presentation titled "Security Overview," detailing other cybersecurity incidents.

106. Also, in connection with Marriott's February 12, 2016 meeting of the Board (a mere seven months before the Merger closed), Defendant Oberg provided a slide presentation to the entire Board, which included the Audit Committee Defendants and Defendant Sorenson. The presentation included a slide titled "Overall Company Risk Ranking" that ranked the top risks facing Marriott in 2016. One slide demonstrated that the Board itself ranked cybersecurity as the number one risk Marriott faced in 2016. Another slide showed that "the Board of Directors and

Management both view [cybersecurity] risk as having increased from 2015 to 2016" and "[c]ybersecurity is an enterprise-wide risk that continues to make headlines and present challenges for many large organizations due to the sophistication of cyber events and the related costs . . . . Large-scale cybersecurity breaches can quickly erode customer confidence and result in significant brand damage."

107. Also, during this February 12, 2016 Board meeting, the Director Defendants were provided the results of a survey of 270 of Marriott's top executives which included a slide titled "OVERALL TOP 5 RISKS: IMPACT ASSESSMENT." This slide revealed that 59% of these executives considered cybersecurity as a "High/Substantial" risk. Another slide titled "OVERALL TOP 5 RISKS: EFFECTIVENESS ASSESSMENT" demonstrated management's assessment of the effectiveness of the risk mitigation activities for the top five risks facing the Company. Regarding cybersecurity it revealed that 38% of the executives believed that Marriott's mitigation plans to address the cybersecurity risk should be "significantly enhanced" or "enhanced," and another 38% responded that "certain areas could be enhanced to more fully address the risk."

108. A July 18, 2016 internal report titled "Marriott IT Infrastructure & Security Business Cases" discussed integration of the Marriott Loyalty Rewards and Starwood Preferred Guest databases through 2018 and a cost summary of this infrastructure. The report cautioned that the Starwood preferred guest database did not have a Security Incident & Event Management ("SIEM") process in place to identify, monitor, and analyze IT-security events in real time:

> Starwood does not currently have a SIEM. The SIEM is the method by which an organization can leverage system and application logs to identify anomalies in the environment that could be indicators of compromise. Not having a SIEM would result in security events going undetected.

109. The July 18, 2016 report also reported that Starwood did not monitor and report on the company's "state of security," and did not have visibility into its out-of-date operating systems,

including whether malware was running on those systems. Further, the report revealed that Starwood did not use tokenization or point-to-point encryption on its systems. Consumer Complaint at ¶¶ 124-126. Although Plaintiffs do not know whether the Director Defendants received this report, these defendants received at least some of this information (Starwood's failure to use tokenization or point-to-point encryption) from Defendant Hoffmeister on February 10, 2017.

110. Documents also demonstrate that Defendants were repeatedly informed of the threat of a cybersecurity incident throughout the Relevant Period, while they were touting the supposed "extensive due diligence" Marriott was conducting. About three months after the close of the Merger, at a December 2016 meeting among the Audit Committee Defendants, the Company's Independent Registered Public Accounting Firm ("External Auditor"), Ernst & Young ("E&Y"), reminded the Audit Committee that "[w]hile cybersecurity has historically been a topic of discussion in board rooms, the increase in the volume and severity of attacks, coupled with the increased scrutiny by regulators, has significantly elevated its importance."

111. The Board and its committees, including the Audit Committee Defendants, met again on February 8, 2017. The Audit Committee Defendants were informed by their External Auditor, E&Y, that the Audit Committee was "now expected to have an understanding of the business implications of cyber risks" and that "cybersecurity has emerged to prominence as a massive risk area for the hospitality industry," as well as the appropriateness of the Company's risk disclosures related to cybersecurity. Even Marriott's own internal Audit Department rated Marriott as "Needs Improvement" in cybersecurity.

112. Two days later, on February 10, 2017, Defendant Sorenson and the Audit Committee Defendants were reminded about the level of cybersecurity risk facing Marriott,

including through a presentation on data breaches in the hospitality industry. Importantly, Defendant Sorenson and the Audit Committee Defendants were explicitly informed of the cybersecurity risks involving Starwood's legacy systems—including risks regarding the database still in use after the Merger. PwC, Marriott's consultant, was brought in to present on this topic to the Board and explained that Starwood's "[b]rand standards did not mandate PCI [*i.e.*, Payment Card Industry] compliance, tokenization, or point-to-point encryption." Importantly, Marriott was contractually required to be PCI compliant because of its role as credit card processor. Further, being PCI compliant required encryption of credit card information, *e.g.*, tokenization or point-to-point encryption. Point-to-point encryption means card data is encrypted immediately upon use. Also, tokenization is the process of replacing payment card data with a non-sensitive equivalent, such as a string of random numbers and characters. Without encryption, credit card numbers were readily observable to anyone accessing Starwood's network—a massive security flaw. Thus, the Board, including Defendant Sorensen and the Audit Committee Defendants, were specifically informed on February 10, 2017, that credit card information on Marriott's systems was extremely vulnerable to theft and that Starwood's systems were non-compliant with standards Marriott was contractually obligated to follow. Importantly, Defendants Oberg and Hoffmeister were also present at that meeting. Yet, Defendants did nothing in response. PwC also reported that Starwood's "[d]ecentralized technology management model created a different risk profile than Marriott's centralized approach" which "[a]llowed for greater opportunity for deviation from the expected published standard, and led to an unusually high number of associates with elevated access to systems." Defendant Sorenson and the Audit Committee Defendants would have known all of this if a proper due diligence investigation was conducted at the time of the Merger and thereafter. Further, if Defendants did not know before the February 2017 Board meeting, they

definitely knew that Starwood was not compliant with the Payment Card Industry Data Security Standard ("PCI DSS") as of this date. Importantly, according to confidential witnesses in the Securities Complaint (discussed herein at ¶¶ 128 and 493) and pleadings filed in parallel litigation discussed herein at ¶ 231), Marriott protected its own systems using tokenization.

113. Finally, in August 2018, Defendant Sorenson and the Board, including the Audit Committee Defendants, were informed that Marriott found "[m]alware on a legacy-Starwood server used by the Marriott Law Department back in January 2018." And at the same August 2018 meeting of the Board, Defendant Sorenson and the Audit Committee Defendants learned about additional security incidents, including a malicious legacy-Starwood domain registered in September 2017. Still, Defendants did nothing to improve cybersecurity controls in its legacy Starwood system, and disclosed nothing to the market/investors.

114. Additionally, Defendants Sorenson, Oberg, Bauduin, Hoffmeister and the Audit Committee Defendants (Bush, Henderson, Lewis, Kellner, and Muñoz) had access to several reports and assessments throughout the Relevant Period detailing the deficiencies in Starwood's systems. For example, a Marriott internal report dated July 18, 2016—a date just under two months before the Merger closed (and more than eight months after the Relevant Period started)—detailed significant issues with Starwood's systems, including that Starwood lacked a Security Incident Event Management ("SIEM") process, did not monitor or report on the "state of security" of its systems, and did not use tokenization or point-to-point encryption. In January 2017, PwC informed Marriott of the results of PwC's "Starwood Cybersecurity Assessment," which detailed several critical vulnerabilities in Starwood's systems, including that Starwood: (1) lacked an enterprise-wide security governing body; (2) lacked adequate network segmentation; (3) consistently failed to comply with baseline configuration standards, leaving the systems

vulnerable; and (4) did not mandate PCI DSS compliance.

115. Defendants knowingly and/or recklessly ignored the above assessments, recommendations, and warnings about Starwood's cybersecurity issues for at least a year after the February 10, 2017 disclosure. On February 9, 2018, the Board had a meeting attended by Defendants J.W. Marriott, Bush, Duncan, Harrison, Henderson, Hippeau, Kellner, Lee, Lewis, Muñoz, Reinemund, Schwab, and Sorenson (and former director Romney). They received the CFO's Report which listed cybersecurity as "a Top Five Risk for Overall Company and the Board of Directors." The Director Defendants also received a presentation that listed "Key Mitigating Activities" Marriott was supposedly undertaking with respect to the Company's top five risks. This list did not include any effort to update Starwood's systems. During this meeting, the Director Defendants were told that for the past year, Marriott had elected to simply "[i]mplement[] patching" to fix issues related to Starwood's unsafe databases, and that the transition and "[m]igration of Starwood systems to the Marriott established technology standards for PCs, Laptops and other end user devices" would not be completed until September, 2019.

116. On August 9, 2018 the Director Defendants were informed that Marriott found "[m]alware on a legacy-Starwood server used by the Marriott Law Department" back in January 2018. During this meeting, the Director Defendants were also informed of additional security events or incidents, including a malicious legacy Starwood domain registered in September 2017.

**(4) The Merger**

117. On November 16, 2015, Marriot filed a Form 8-K with the SEC and issued a joint press release with Starwood announcing that ". . . the boards of directors of both companies have unanimously approved a definitive merger agreement under which the companies will create the world's largest hotel company."

118. On information and belief, Plaintiffs allege that in an acquisition of this complexity and size, it is standard practice to perform cybersecurity due diligence, including researching undisclosed or unknown data breaches, as well as identifying information technology security risks and weaknesses in operations and governance of the target company. In this case, it was a primary responsibility of Defendants to perform a full and complete cyber-security assessment to understand the state of Starwood's computer networks, systems, and its vulnerabilities.

119. On the heels of this merger announcement, on November 20, 2015, Starwood disclosed that more than 50 of its hotels had been infected by a malware attack designed to help cyber thieves steal credit and debit card data (the "2015 Starwood Data Breach"). As a result of the malware attack, unauthorized parties were able to access certain payment card data belonging to Starwood customers, which included payment card numbers, names of cardholders, expiration dates, and card security codes.

120. The 2015 Starwood Data Breach and disclosure is separate and distinct from the Data Breach disclosed by Marriott on November 30, 2018. As stated in a 2015 *Krebs on Security* article[8]:

> Starwood Hotels & Resorts Worldwide today warned that malware designed to help cyber thieves steal credit and debit card data was found on point-of-sale cash registers at some of the company's hotels in North America. ***The disclosure makes Starwood just the latest in a recent string of hotel chains to acknowledge credit card breach investigations, and comes days after the company announced its acquisition by Marriott International***. [Emphasis added]

121. The 2015 Starwood Data Breach is another Red Flag.

122. On December 22, 2015, Marriott filed its Form S-4 with the SEC (the "2015 Proxy"), which asked for shareholder vote approving the Marriott/Starwood merger. In the 2015

[8] This November 20, 2015 article titled "Starwood Hotels Warns of Credit Card Breach" can be found at https://krebsonsecurity.com/2015/11/starwood-hotels-warns-of-credit-cardbreach/ (Last visited Aug. 4, 2020).

Proxy, both companies recommended that their shareholders vote for the then-proposed merger. When discussing risk factors, the 2015 Proxy was silent on the 2015 Starwood Data Breach, or more generally, risks associated with Technology, Information Protection, and Privacy Risks.[9] The 2015 Proxy does not mention or discuss "personal information", "PCD", "PII", or the data breaches discussed herein.

123. On January 27, 2016, Marriott filed its Form S-4/A with the SEC (the "2015 Proxy Amendment 1") which asked for shareholder vote approving the Marriott/Starwood merger. On February 16, 2016 Marriott filed its Form S-4/A with the SEC (the "2015 Proxy Amendment 2") which also asked for shareholder vote approving the Marriott/Starwood merger. Neither of these Proxy Statements mentioned or discussed "personal information", "PCD", "PII", or the data breaches discussed herein.

124. On September 23, 2016, Marriott filed a Form 8-K with the SEC and issued a press release announcing that it had completed its acquisition of Starwood. At that same time, Marriott announced it had expanded its Board of Directors from eleven (11) to fourteen (14) and added former Starwood directors to the Marriott Board; namely, Defendants Duncan, Hippeau, and Lewis. Through the Merger, Starwood shareholders received $21.00 in cash and 0.800 shares of Marriott common stock, for total consideration of $13.6 billion. Following the Merger, Marriott is the largest multinational chain of hotels in the world

125. On September 23, 2016, Starwood also updated its Online Privacy Statement. In defining Starwood's mission, it states that Starwood is ". . . dedicated to protecting your privacy and safeguarding your personal data." Under "Security Safeguards", Starwood goes on to state:

Starwood recognizes the importance of information security, and is constantly

[9] The 2015 Proxy, under "Risks Related to Starwood's (and separately, Marriott's) Business", refers interested parties to each company's Form 10-K to seek out additional risk information. Buried therein is limited disclosure of cyber threats.

> reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your personal data against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls" and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.

126. Following the completion of the Merger, Marriott kept the loyalty programs for each brand (Marriott and Starwood) separate. On information and belief, this resulted in Marriott taking control, responsibility, and use of the Starwood database which was at the heart of the Data Breach. As stated in an April 18, 2018 *Forbes* article titled "Details Surrounding the Marriott and Starwood Merger":

> In the beginning, Marriott chose to keep loyalty programs for the two hotel brands completely separate; that is, customers could book Marriott hotels with Marriott Rewards Points and Starwood hotels with SPG Starpoints. Additionally, members had the opportunity to link both accounts in order to enjoy elite status in both programs and switch between point currencies at an exchange rate of one SPG Starpoint for every three Marriott Rewards Points. This pleased Starwood account holders, as it respected the value of SPG Starpoints and made sure that the merger would work for both parties.
>
> Upon closing, the plan was to eventually build a newer, stronger loyalty program that played to the strengths of each one. "Marriott will draw upon the very best each program offers and we can't wait to show the loyal members of these programs the power and benefits of Marriott and Starwood coming together," explains Executive Vice President and Global Chief Commercial Officer Stephanie Linnartz.

127. After completion of the Merger, Marriott hosted the Starwood guest reservation database on Marriott-owned hardware in a data center operated by Digital Realty in Phoenix, Arizona. Accenture continued managing the operation of the Starwood guest reservation database, as it had since late 2009. Although Marriott assured the investing public that the integration was well underway while touting the Company's sophisticated technology and reservation systems.

After the Merger, these technologies and systems included Starwood's own dangerously vulnerable Oracle application which remained unsecure and open for cyber-attacks. Marriott failed to disclose these material factors, further shrouding the Company's own susceptibility to heightened cyber risks.

128. As recounted and more fully described in the Securities Complaint, former Marriott and/or Starwood employees (identified as "CWs") provided evidence of identified Starwood IT weaknesses and problems. As detailed therein, these weaknesses and problems were identified through pre-merger due diligence and post-merger integration efforts. Defendants knew of these problems and weaknesses. By way of example:

(a) CW 2, who was employed as a Senior Global Cyber-Security Consultant at Starwood from September 2014 to December 2015, explained that Starwood used a very antiquated version of the Oracle application portal for its IT system, which contained over 150 applications, including the Starwood's Reservation and SPG Loyalty Points systems. He explained that Starwood refused to pay Oracle for maintenance support for years, so "nothing was updated or patches implemented to prevent hacking." This former Starwood consultant also said this left Starwood's Oracle application portal seven years past its end of life and very vulnerable to attack by hackers (*see* Securities Complaint, ¶¶ 13, 154)

(b) CW 5, who was employed by Marriott as a Senior Director from the start of the Relevant Period through early 2017, stated that Starwood's Oracle stack would have cost hundreds of millions of dollars to fix, and that this was Starwood's main reason for agreeing to the merger with Marriott. CW 5 further confirmed that Marriott was aware of this.

(c) CW 2 stated that Starwood was aware of the problems with their databases

but did not "want to spend $10-$20 million on a system rollout." CW 2 claimed that Starwood instead opted to go "on the cheap" with an encryption program that merely slowed, rather than stopped potential hackers from gaining access to Starwood customers' passwords.

(d) Defendant Sorenson was personally involved with Marriott's acquisition of Starwood. Defendant Sorenson was Marriott's point person during Marriott's initial interest in Starwood, Marriott's decision to reengage with the acquisition process, and Marriott's ultimate decision to acquire Starwood. As detailed in prospectuses filed related to the Merger, Defendant Sorenson held numerous individual meetings with Starwood executives during the acquisition process. Additionally, ***Defendant Sorenson was a member of the Board and met repeatedly with the Company's Board to keep them informed of the process***. The prospectus also states that the Board, of which Defendant Sorenson was a member gained an enhanced "understanding of the integration process" with the addition of the former Starwood board members. The prospectus also stated that the Board's review of the due diligence process gave it a "favorable" outlook for the Merger. (Emphasis added).

(e) CW 1, who worked at Marriott as a Software Developer and Technical Lead from 2005 through 2018, explained that ***Marriott had traditionally performed two different audits of their IT systems annually***, one focused on PCI compliance and the other focused on System Organizational Controls driven by SOX. CW 1 also said that ***in March 2016, he attended a presentation about a third, unexpected audit*** that was conducted. He found out at that presentation that ***the third audit had been commissioned by the Board of Director's Audit Committee***. He advised that this third audit was similar to the other two

audits in that PWC, the auditors, collected random samplings of data and did their own discovery work. ***According to CW 1, vulnerabilities with Marriott's business IT systems including exposure to the internet and issues related to the guest system were identified by this third audit and presented in March 2016. CW 1 said that everyone was aware of the findings from the third audit, including the Board of Directors, Defendant Sorensen and Defendant Hoffmeister. CW 1 added that they also knew that Starwood's IT system was even worse.*** CW 1 advised that the PWC auditors were checking for vulnerabilities in Marriott's system and that they attached all different aspects of the systems to perform this audit. (Emphasis added).

129. Thus, Marriott's approach to the Starwood IT deficiencies was a blatant departure from the Company's previous diligent IT security approach. A s the Company shifted its leadership in 2016, Marriott's due diligence efforts continued to falter with IT security issues. Contrary to the Company's representations concerning the diligent and appropriate handling of the Integration, the reality was a far cry. Indeed, the Director Defendants, including the Audit Committee Defendants, were privy to numerous red flags during the Relevant Period, including yet another data breach in September 2017 of Equifax that affected almost 150 million individuals and subjected Equifax to numerous lawsuits and regulatory actions, including a $525-$700 million settlement with the FTC, the Consumer Financial Protection Bureau, and 50 U.S. states and territories related to the aforementioned data breach.

130. The Starwood IT weaknesses and problems identified during the pre-merger due diligence and post-merger integration were red flags.

131. Defendants knew, should have known, and/or recklessly disregarded the identified red flags when it proceeded with the Merger, its integration efforts of Starwood systems post-

merger, when Defendants made the false and misleading statements, and caused the Company to repurchase stock, as alleged herein. Defendants benefitted from ignoring these red flags by participating in insider transactions, as alleged herein.

**C. The Data Breach**

132. On September 8, 2018, Marriott's IT team learned of the Data Breach after being notified by the Company's third-party IT contractor, Accenture. Accenture was tasked with managing Starwood's reservation database. The breach was first identified by a technology tool called "Guardium" the day before. Defendant Sorenson, in his March 7, 2019 testimony before the Senate Committee on Homeland Security & Governmental Affairs, Permanent Subcommittee on Investigations described how Marriott learned of the Data Breach, stating:

> On September 8, 2018, Accenture, which managed the Starwood Guest Reservation Database, contacted Marriott's IT team with information about a Guardium alert generated on September 7. Guardium is an IBM security product used on the Starwood system to help secure databases. The Guardium alert was triggered by a query from an administrator's account to return the count of rows from a table in the database.

133. Defendants were informed of identified malware relating to the Data Breach not later than September 18, 2019, as evidenced by Defendant Sorenson's congressional testimony where he stated:

> On September 10, 2018… Marriott brought in third-party investigators to conduct a full investigation into the circumstances that led to the alert and to assist with containment measures. On September 17, 2018, the investigators uncovered a Remote Access Trojan ("RAT"), a form of malware that allows an attacker to covertly access, surveil, and even gain control over a computer. I was notified of the ongoing investigation that day, and ***our Board was notified the following day***. [Emphasis added]

134. In Defendant Sorenson's congressional testimony, he further disclosed that "…there was evidence of an unauthorized party on the Starwood network since July of 2014…". He also confirmed that the investigators found evidence of malware, including MimiKatz, a tool

that searches a device's memory for usernames and passwords.

135. In Defendant Sorenson's congressional testimony, he claimed that on November 13, 2018 its investigators identified evidence that two compressed, encrypted files had been deleted from a device that they were examining and removed from the Starwood network, although the contents of those files were allegedly not known at that time. He further claimed that on November 19, 2018 the investigators were able to decrypt the files and determine that one was from the Starwood Guest Reservation Database and contained guest data and the other contained passport information. Marriott was aware in early November of 2018 that the Data Breach stemmed back to at least mid-2014. During that time, the Company implemented "endpoint detection technology on devises across the Starwood network."

136. In his congressional testimony, Defendant Sorenson also disclosed:

> [W]e found that, in 2015 and 2016, prior to our acquisition of Starwood, the attacker had likely created a copy of two other tables, which the attacker later deleted. The file names correspond to two other tables in the Starwood Guest Reservation Database. We have been unable to recover those files and could not determine if they had been taken.

137. Defendants did not provide notice of the Data Breach to certain interested entities until November 29, 2018; namely, 83 days after Defendants discovered the Data Breach, the Company sent notices out to four major credit card networks and their vendors in more than 20 countries and territories. The Company also provided the FBI with an update and notified state Attorneys General, the FTC, and the SEC, among other entities. The following day, approximately 3 months after the fact, the Company publicly disclosed the Data Breach. Significantly, data breaches on average, last about 266 days before they are identified and contained—the Data Breach concerning Starwood however (and Marriott) continued undisturbed for over for more than 1,500 days from evidence of the first intrusion, including more than 700 days while under Marriott's

ownership and control.[10]

138. On December 11, 2018, Defendants finished notifying all of its U.S.-based guests that the Data Breach had occurred. Defendants did not disclose whether the information stolen by the attackers had included encryption keys.

139. This Data Breach would later be described as ". . . one of the biggest data breaches on record".[11] On November 30, 2018, Cowen Inc. issued an analyst report commenting on the Data Breach. In relevant part, the analyst report stated that the Data Breach "may hamper loyalty enrollment," and had caused "real brand damage."

140. In breach of their fiduciary duties, Defendants knowingly or recklessly caused the Company to permit the Data Breach to continue until approximately September 2018 and/or failed to identify the existence of the Data Breach, despite Defendants' assurance that it sought to use reasonable measures to protect the Company's customers' personal information. As a result of the Data Breach, Defendants caused the Company to expose customer data to third parties without authorization, indicating that the Company had lax or non-existent data and security policies and protocols, and that the Company's security systems were ultimately inadequate to protect customer data.

141. Defendants were – and at all relevant times have been – aware that PII collected by the Company is highly sensitive and could be used for illicit and nefarious purposes by third parties, including perpetuating identity theft and engaging in fraudulent transactions.

142. Beyond their general duties to ensure effective systems are in place to protect customers' information to prevent the risk of loss, Defendants were – and at all relevant times have

---

[10] *See* Rob Sobers, *Data Breach Response Times: Trends and Tips*, Varonis (Mar. 13, 2019).

[11] *See* November 30, 2018 Chicago Tribune article, "Marriott security breach exposed data of up to 500 million guests", at https://www.chicagotribune.com/business/ct-marriott-data-breach-20181130-story.html. (Last visited Aug. 4, 2020).

been – obligated to oversee the Company's compliance with rules governing payment card transactions and PII, industry standards and various federal and state laws, in addition to the Company's own internal policies, procedures, and commitments.

143. Defendants have long been aware of the risk of cyber-attacks, especially following Target's notorious data breach in 2013.

144. The Company's Form 10-K for the fiscal year ended December 31, 2014, filed before the Merger was announced stated:

> *Failure to maintain the integrity of and protect internal or customer data could result in faulty business decisions, operational inefficiencies, damage to our reputation and/or subject us to costs, fines, or lawsuits*. Our businesses require collection and retention of large volumes of internal and customer data, including credit card numbers and other personally identifiable information of our customers in various information systems that we maintain and in those maintained by third parties with whom we contract to provide services, including in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. We and third parties who provide services to us also maintain personally identifiable information about our employees. The integrity and protection of that customer, employee, and company data is critical to us. If that data is inaccurate or incomplete, we could make faulty decisions. Our customers and employees also have a high expectation that we and our service providers will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems or our franchisees' systems may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our and our service providers' information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our franchisees or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits

145. The Company's Form 10-K for the fiscal year ended December 31, 2015, filed before the Merger was completed stated:

> *Cyber-attacks could have a disruptive effect on our business.* Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records. Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits. In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.

146. Substantially similar risk disclosures were repeated in both the 2016 and 2017 10-Ks.

147. The Company's Board bears responsibility for risk oversight, including the oversight of cybersecurity risks. As articulated in the 2018 Proxy Statement:

> The Board of Directors is responsible for overseeing the Company's processes for assessing and managing risk. The Board considers our risk profile when reviewing our annual business plan and incorporates risk assessment into its decisions impacting the Company. In performing its oversight responsibilities, the Board receives an annual risk assessment report from the Chief Financial Officer and discusses the most significant risks facing the Company. ***As part of this annual review, the Board reviews the Company's cybersecurity risk profile and is informed on the specifics of the cybersecurity risk program in a separate annual presentation by the Company's Chief Information Officer. This program provides the Board with an overview of the cybersecurity risks and threats landscape as well as reviews the Company's risk posture. The Board is further briefed on actions and changes taken by management to mitigate the Company's risk profile and provided with an overview of the cybersecurity strategy along with key cybersecurity initiatives and incidents.*** [Emphasis added]

148. The 2018 Proxy Statement further notes that the Audit Committee and the

Compensation and Policy Committee play important roles in risk management:

> The Board also has delegated certain risk oversight functions to the Audit Committee. In accordance with its charter, the Audit Committee periodically reviews and discusses the Company's business and financial risk management and risk assessment policies and procedures with senior management, the Company's independent auditor, and the Chief Audit Executive. The Audit Committee incorporates its risk oversight function into its regular reports to the Board.
>
> In addition, the Compensation Policy Committee reviewed a risk assessment to determine whether the amount and components of compensation for the Company's associates and the design of compensation programs might create incentives for excessive risk-taking by the Company's associates. As explained in the CD&A below, the Compensation Policy Committee believes that our compensation programs encourage associates, including our executives, to remain focused on a balance of the short- and long-term operational and financial goals of the Company, and thereby reduces the potential for actions that involve an excessive level of risk.

149. However, as would later be revealed on November 30, 2018, in breach of their fiduciary duties, Defendants knowingly or recklessly caused the Company to permit the Data Breach to continue until approximately September 2018 and/or failed to identify the existence of the Data Breach. Defendants failed to conduct adequate due diligence in connection with the Merger, causing them to fail to discover that a security vulnerability existed in Starwood's guest reservation database in the United States. As a result of said vulnerability, certain actors had gained unauthorized access to Starwood's network since 2014. In further breach of their fiduciary duties, Defendants made or caused the Company to make the false and misleading statements below concerning, *inter alia*, the Data Breach, Merger, Marriott's due diligence, and the Integration.

### D. Data Security Rules and Regulations

150. Whether performing its core operations, which includes gathering its customers personal data, or participating in acquisitions of other hotel companies, Marriott is required to comply with a variety of laws, rules, and regulations discussed below.

**(1) Payment Card Industry Data Security Standard ("PCI DSS")**

151. PCI DSS is a set of security standards for organizations that handle branded credit cards from the major credit card companies. The standards are designed to protect the sensitive information involved in processing payments. PCI DSS applies to any organization, including Marriott, that accepts, transmits, or stores any cardholder data.

152. The Payment Card Industry Security Standards Council ("PCI SSC") was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry ("PCI") security standards with a focus on improving payment account security throughout the transaction process. The PCI DSS[12] is administered and managed by the PCI SSC an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB).

153. PCI SSC invites organizations (referred to as "Participating Organizations") to become a PCI stakeholder:

> Participating Organizations have the opportunity to have their voices heard about our standards via the Request for Comment (RFC) process. Additionally, Participating Organizations can attend community meetings, receive exclusive Council communications, such as advance review of drafts of standards and supporting materials, and regular dialogue with key stakeholders. With more than 750 organizations from across industries and around the world, including retailers, airlines, hotels, banks, technology companies, payment processors and industry associations, these organizations play a key role in both influencing the ongoing development of PCI Security Standards and programs, and in helping ensure that PCI Security Standards are implemented globally to secure payment data.[13]

154. At all relevant times, Marriott was a Participating Organization of PCI DSS, and because of this membership, it was fully aware of the PCI DSS requirements and had an opportunity to review them and provide feedback.

---

12 www.pcisecuritystandards.org.

13 https://www.pcisecuritystandards.org/get_involved.

155. PCI DSS sets requirements detailing how companies protect, store, and transmit data. For example, companies are required to establish and implement firewalls that control entry to and exit from the network and block unwanted access. As an additional example, pursuant to PCI DSS requirements companies are required to prevent unauthorized outbound traffic from the cardholder data environment to the Internet. The PCI DSS standards and requirements put the responsibility on the company to design effective data security procedures. Marriott has been subject to these requirements since 2004.

156. PCI DSS publishes its resource, PCI Data Security Standard Requirements and Security Assessment Procedures, which states: "PCI DSS comprises a ***minimum*** set of requirements for protecting account data." (Emphasis added). It includes an overview of the PCI DSS requirements:

**PCI Data Security Standard – High Level Overview**

| | |
|---|---|
| **Build and Maintain a Secure Network and Systems** | 1. Install and maintain a firewall configuration to protect cardholder data<br>2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | 3. Protect stored cardholder data<br>4. Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | 5. Protect all systems against malware and regularly update anti-virus software or programs<br>6. Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | 7. Restrict access to cardholder data by business need to know<br>8. Identify and authenticate access to system components<br>9. Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | 10. Track and monitor all access to network resources and cardholder data<br>11. Regularly test security systems and processes |
| **Maintain an Information Security Policy** | 12. Maintain a policy that addresses information security for all personnel |

157. As set forth in PCI DSS requirements and security assessment procedures, these 12 requirements include between 2 and 10 subsections that set forth detailed technical controls. Credit card merchants and processors are also required to hire Qualified Security Assessors ("QSAs") to independently verify and validate evidence that all requirements are met.

**(2) FTC Act**

158. Marriott is required to comply with Section 5 of the FTC Act (15 U.S.C. § 45) which states in part that ". . . unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." Unfair or deceptive acts or practices in or affecting commerce includes data security. In the Memorandum Opinion when ruling on Marriott's Motion to Dismiss in the Consumer Track (ECF 540), this Court found that "Section 5 of the FTC Act is a statute that creates enforceable duties. Moreover, this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context."

159. The FTC has issued various resources for business, highlighting the importance of reasonable data security practices.[14] One of these resources, published in June 2015, is titled "Start with Security, a Guide for Business – Lessons Learned from FTC Cases" ("Start with Security"). Start with Security lists and discusses 10 guidelines gleaned from past FTC enforcement actions. The topics covering these guidelines are:

- Start with security. Factor it into the decision making in every department of your business;
- Control access to data sensibly;
- Require secure passwords and authentication;
- Store sensitive personal information securely and protect it during transmission;
- Segment your network and monitor who's trying to get in and out;
- Secure remote access to your network;
- Apply sound security practices when developing new Products;
- Make sure your service providers implement reasonable security measures;
- Put procedures in place to keep your security current and address vulnerabilities that may arise; and

[14] *See* https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security. Last visited August 17, 2020.

- Secure paper, physical media, and devices.

160. In Start with Security, Topic 9 begins with the FTC's unequivocal language – "Outdated software undermines security. The solution is to update it regularly and implement third-party patches."

161. On December 17, 2015 and in its enforcement action against LifeLock, the FTC stated ". . . PCI DSS certification is insufficient in and of itself to establish the existence of reasonable security protections." Referring to the FTC's enforcement action against Wyndham Worldwide Corporation ("Wyndham") this statement also provides: "The Wyndham order calls for a number of additional significant protections, including the implementation of risk assessments, certification of untrusted networks, and certification of the assessor's independence and freedom from conflicts of interest."

162. The Wyndham enforcement action is instructive. In three separate data breach incidents in 2008 and 2009, Wyndham was hacked when Wyndham's customer data was accessed by hackers via a local network at a hotel and also using an administrative account in the Wyndham data center. The FTC initiated an enforcement action on June 26, 2012, for violations of the FTC Act including unfair and deceptive practices. In its December 11, 2015 settlement with Wyndham, as a result of these data breaches, the FTC provided guidance on conducting risk assessments and monitoring internal safeguards and controls -- basically a road map for hotel companies to assess their own cybersecurity measures. In a December 9, 2015 FTC press release discussing the Wyndham settlement, FTC Chairwoman Edith Ramirez stated, "This settlement marks the end of a significant case in the FTC's efforts to protect consumers from the harm caused by unreasonable data security".

163. On August 31, 2016, the FTC also published a blog post endorsing the National

Institute of Standards and Technology ("NIST") and its Cybersecurity Framework (the "Framework"), answering the question: "If I comply with the NIST Cybersecurity Framework, am I complying with what the FTC requires?" In response, Andrea Arias (on behalf of the FTC) stated:

> From the perspective of the staff of the Federal Trade Commission, NIST's Cybersecurity Framework is consistent with the process-based approach that the FTC has followed since the late 1990s, the 60+ law enforcement actions the FTC has brought to date, and the agency's educational messages to companies, including its recent Start with Security guidance
>
> * * *
>
> The types of things the Framework calls for organizations to evaluate are the types of things the FTC has been evaluating for years in its Section 5 enforcement to determine whether a company's data security and its processes are reasonable. By identifying different risk management practices and defining different levels of implementation, the NIST Framework takes a similar approach to the FTC's long-standing Section 5 enforcement.

164. In October 2016, the FTC published "Protecting Personal Information – A Guide for Business" which established guidelines for fundamental data security principles and practices for business (the "PPI Guidelines").

165. In the PPI Guidelines the FTC states that businesses should protect the personal customer information it keeps; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct security problems.

166. In the PPI Guidelines, the FTC also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

167. In the PPI Guidelines the FTC also recommends that companies limit access to

sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

**(3) National Institute of Standards and Technology ("NIST") and its Cybersecurity Framework ("Framework")**

168. In the NIST's publication, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (April 16, 2018), the Executive Summary states in relevant part:

> The United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the Nation's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects a company's bottom line. It can drive up costs and affect revenue. It can harm an organization's ability to innovate and to gain and maintain customers. Cybersecurity can be an important and amplifying component of an organization's overall risk management.
>
> To better address these risks, the Cybersecurity Enhancement Act of 2014 (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. Through CEA, NIST must identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."

169. NIST organizes its approach into three components: (1) Framework Core; (2) Framework Implementation Tiers; and (3) Framework Profile.

170. The Framework Core provides a set of activities to achieve specific cybersecurity outcomes, and it references examples of guidance to achieve those outcomes. The Core is comprised of four elements: Functions, Categories, Subcategories, and Informative References. Functions organize basic cybersecurity activities at their highest level. These Functions are (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.

171. The Framework Implementation Tiers ("Tiers") provide context on how an

organization views cybersecurity risk and the processes in place to manage that risk. In the Framework, the Tiers are described: as Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). Each Tier describes an increasing degree of rigor and sophistication in cybersecurity risk management practices.

172. NIST encourages organizations to manage its cybersecurity risk at Tier 2 ("Risk Informed") or greater. The cybersecurity expert used by the plaintiffs in the Securities Class Action determined that the risk management capability within Marriott's cybersecurity program would be classified in the "Partial" tier (Tier 1) and would therefore be insufficient. This is because "Risk Informed" (Tier 2) implies that prioritization, and management of protect, detect, and respond activities, is based on the outcome of formal risk assessment informed by threat intelligence and situational awareness, and the PFI Report shows that Marriott did not exhibit such awareness.

173. As stated in its publication, the Framework Profile "is the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. A Profile enables organizations to establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities."

**(4) GDPR**

174. Marriott is also required to comply with GDPR, which is a European regulation requiring data protection and privacy for all individuals within the European Union ("EU") and the European Economic Area. GDPR became effective on May 25, 2018 and regulates the storage, transmission, and processing of personal information of EU residents. Violations of GDPR can subject a company to a fine of up to 4% of its annual global revenue.

175. Marriott is subject to the GDPR because it collects data from EU residents. For the purposes of GDPR, Marriott is considered both a data processor and a data controller. The GDPR defines data controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" and data processor as the "natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller", such as the hotels managed by Marriott.

176. The Information Commissioner's Office ("ICO") is responsible for enforcing the GDPR and is leading an investigation into the Data Breach. As detailed in the Consumer Complaint, in Marriott's December 6, 2018 response to the ICO, it admitted that the merger "transaction did not trigger any change in the nature and scope of the personal data processing activities related to the Starwood Guest Reservation Database, and Marriott had no reason to conclude that the transaction was likely to result in a high risk to the rights and freedoms of individuals. In that context, Marriott did not produce any formal data protection impact assessment in relation to its acquisition of Starwood."

177. On July 9, 2019, the ICO issued a notice of its intention to fine Marriott International £99,200,396 (approximately $123 million) for infringements of the General Data Protection Regulation. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems. Information Commissioner Elizabeth Denham stated in relevant part

> The GDPR makes it clear that organizations must be accountable for the personal data they hold. This can include carrying out proper due diligence when making a corporate acquisition and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected.
>
> Personal data has a real value so organizations have a legal duty to ensure its security, just like they would do with any other asset. If that doesn't happen, we will not hesitate to take strong action when necessary to protect the rights of the

public.

**(5) Safe Harbor and Privacy Shield Frameworks**

178. Defendants caused Marriott to inform the public through its website www.starwoodhotels.com that the Company's data security practices were compliant with the U.S.-EU Safe Harbor Framework ("Safe Harbor Framework"). Defendants also caused Marriott to inform the public through www.Marriott.com that the Company followed the data security requirements set forth in the EU-U.S. Privacy Framework and the Swiss-U.S. Privacy Shield Framework (collectively the "Privacy Shield Frameworks"). These standards have been superseded by GDPR.

179. The Safe Harbor Framework was in effect until 2015 and was designed to assist U.S. companies that process personal data collected in the EU in complying with European privacy regulations. The Safe Harbor Framework has seven requirements companies must adhere to in order to attest compliance: (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement.

180. The EU-U.S. Privacy Shield Framework became effective in 2016, and the Swiss-U.S. Privacy Shield Framework became effective 2017. The Privacy Shield Frameworks were designed to provide American and European countries with a mechanism to comply with European data privacy requirements when transmitting customer data from Europe to the U.S. The Privacy Shield Frameworks have similar requirements to the Safe Harbor Framework.

**(6) COSO Framework**

181. Defendants also caused Marriott to represent in its various Form 10-Ks that the Company used the Internal Control-Integrated Framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (2013 Framework) (the "COSO Framework") to

determine the effectiveness of its internal controls.

182. The COSO Framework was designed to help businesses establish, assess and enhance their internal control and also requires companies to design controls that adequately protect customer data. In the COSO Framework, internal control is composed of: (1) control environment; (2) risk assessment; (3) control activities; (4) information and communication; and (5) monitoring activities.

183. The COSO Framework requirements are process and governance oriented, rather than a set of rules for which controls need to be implemented. COSO has also issued supplemental guidance that is specific to technology controls. This guidance recommends that risk evaluation is aided by comparison of enterprise control activities to technology standards and frameworks that are aligned with the management of cyber risks.

**(7) SEC Guidance**

184. On February 26, 2018, the SEC issued its Statement and Guidance on Public Company Cybersecurity Disclosures (the "Statement"). This Statement provides that "[c]ompanies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity."

185. The SEC requires that companies provide timely and ongoing information in its periodic reports regarding material cybersecurity risks and incidents that trigger disclosure obligations and encourages companies to continue to use Form 8-K or Form 6-K to disclose material information promptly, including disclosure pertaining to cybersecurity matters

186. This Statement also provides:

> Securities Act and Exchange Act registration statements must disclose all material facts required to be stated therein or necessary to make the statements therein not

> misleading. Companies should consider the adequacy of their cybersecurity-related disclosure, among other things, in the context of Sections 11, 12, and 17 of the Securities Act, as well as Section 10(b) and Rule 10b-5 of the Exchange Act.
>
> * * *
>
> In addition to the information expressly required by Commission regulation, a company is required to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading." The Commission considers omitted information to be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available.

187. In discussing "materiality", the Statement provides:

> The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations.33 The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.
>
> * * *
>
> Understanding that some material facts may be not available at the time of the initial disclosure, we recognize that a company may require time to discern the implications of a cybersecurity incident . . . . However, an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.

188. Additionally, when a company experiences a data security incident, the Statement emphasizes the need to "refresh" previous disclosures during the process of investigating a cybersecurity incident or past events.

189. Regarding the form of disclosures, the Statement provides:

> We expect companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents. As the Commission has previously stated, we "emphasize a company-by-company approach [to disclosure] that allows relevant

> and material information to be disseminated to investors without boilerplate language or static requirements while preserving completeness and comparability of information across companies." Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.

190. Regarding a company's risk disclosures in its public filings, the Statement provides in relevant part:

> In meeting their disclosure obligations, companies may need to disclose previous or ongoing cybersecurity incidents or other past events in order to place discussions of these risks in the appropriate context. For example, if a company previously experienced a material cybersecurity incident involving denial-of-service, it likely would not be sufficient for the company to disclose that there is a risk that a denial-of-service incident may occur. Instead, the company may need to discuss the occurrence of that cybersecurity incident and its consequences as part of a broader discussion of the types of potential cybersecurity incidents that pose particular risks to the company's business and operations. Past incidents involving suppliers, customers, competitors, and others may be relevant when crafting risk factor disclosure. In certain circumstances, this type of contextual disclosure may be necessary to effectively communicate cybersecurity risks to investors.

191. Regarding the Board of Directors risk oversight, the Statement provides:

192. Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure. The Commission has previously said that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, this discussion should include the nature of the board's role in overseeing the management of that risk

193. In addition, disclosures regarding a company's cybersecurity risk management

program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.

194. Regarding disclosure controls and procedures, the Statement provides in relevant part:

> Companies should assess whether they have sufficient disclosure controls and procedures in place to ensure that relevant information about cybersecurity risks and incidents is processed and reported to the appropriate personnel, including up the corporate ladder, to enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic information about cybersecurity risks and incidents.
>
> * * *
>
> A company's disclosure controls and procedures should not be limited to disclosure specifically required, but should also ensure timely collection and evaluation of information potentially subject to required disclosure, or relevant to an assessment of the need to disclose developments and risks that pertain to the company's businesses…. Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents.

195. The Statement also cautions companies about insider trading, stating "it is important to have well designed policies and procedures to prevent trading on the basis of all types of material non-public information, including information relating to cybersecurity risks and incidents."

### E. Defendants Knew That Starwood's Systems Were Vulnerable To An Attack Or Were Severely Reckless In Disregarding The Risk -- The Red Flags

196. Defendants ignored red flags that existed at the time of the Merger and thereafter. These red flags should have, and did, put Defendants on notice that Marriott needed to exercise

due care in assessing Starwood's IT systems, and that if Defendants discovered any kind of vulnerability, they needed to immediately remedy the vulnerability to protect the Company's customers' data. These red flags, more fully discussed below, include:

(a) High cybersecurity risks Marriott faced;

(b) Data breaches at various hotels;

(c) Starwood's history of data breaches;

(d) Data breaches at other major corporations; and

(e) Starwood was not PCI DSS compliant and did not use tokenization, or point-to-point encryption.

197. As outlined above, Defendants were explicitly warned of the cybersecurity risks Marriott faced. For example, on February 12, 2016, the Director Defendants received a presentation that ranked the top risks facing Marriott in 2016 which showed that cybersecurity was ranked the number one risk facing Marriott in 2016, and also listed "Information Protection" as a risk. Further, in February 2017, the Audit Committee Defendants and Director Defendants received separate presentations, including an assessment from PwC, informing them that Marriott cybersecurity needs improvement and weaknesses in Starwood's systems. *See* Section VII.B.(3).

198. Hotels have been prime targets of cyber-attacks. The public, including Defendants, learned of the following cyber incidences at the time of each occurrence because it was publicly reported. Defendants also learned of these cyber-attacks either through internal notices (since several involved Marriott hotels), and/or at Board meetings. *See* Sections VII.B.(3), and G. For example:

(a) On February 3, 2014, White Lodging Services Corporation ("White Lodging"), a franchise management company used by Marriott and Starwood, announced

that the point-of-sale ("POS") systems at 14 hotels, including seven Marriott locations, one Westin location, and one Sheraton location, were compromised.

(b) In March 2015, hotel chain Mandarin Oriental Hotel Group confirmed that its hotels were affected by a payment card breach that involved malware.

(c) On April 8, 2015, White Lodging again confirmed that its POS systems at 10 hotels were breached, this time including seven Marriott locations and one Sheraton location.

(d) In November 2015, Noble House Hotels and Resorts announced a breach affecting six of its properties that also involved malware.

(e) On November 20, 2015, Starwood disclosed that it suffered a malware attack at 54 hotels.

(f) On December 23, 2015, Hyatt Hotels Corp. ("Hyatt Hotels") announced that its customers were subject to a data breach through malware the company discovered on its payment processing systems at various properties, including front desks.

(g) In June 2016, Hard Rock Hotel & Casino Las Vegas announced that the resort conducted an investigation revealing that malware had been installed on its servers.

(h) In July 2016, Omni Hotels & Resorts confirmed that a similar malware attack occurred at 49 of its properties

(i) On July 8, 2016, Omni Hotels & Resorts ("Omni Hotels") announced that some of its POS systems had been infected by malware. Omni Hotels revealed that its customers' payment card information was exposed from December 23, 2015 through June 14, 2016. The company stated that more than 50,000 customers' names, card numbers, expiration dates, and CVV numbers across 49 properties were compromised by the breach.

(j) On August 14, 2016, HEI Hotels and Resorts ("HEI") reported that 20 of its hotels, 6 which were operated under the Marriott brand, and 12 which were operated under the Starwood brand, suffered a malware attack, which was active in HEI's system from March 1, 2015 to June 21, 2016, and resulted in a data breach that may have allowed unauthorized parties to access payment card numbers, names of cardholders, expiration dates, and verification codes.

(k) On August 26, 2016, Millennium Hotels & Resorts ("Millennium Hotels") announced that one of its third-party service providers detected "malicious code in certain of its legacy [POS] systems," including those at 14 Millennium Hotels properties. Millennium Hotels revealed the breach affected its food and beverage POS systems.

(l) On September 5, 2016, the Hutton Hotel, in Nashville, TN, announced that its guest reservation system had been infected by malware that compromised customers' names, card numbers, expiration dates, and CVV numbers. The company revealed that the information of guests who placed or paid for a reservation with the Hutton Hotel from September 19, 2012 through April 16, 2015, was at risk.

(m) In September 2016, Kimpton Hotel & Restaurant Group LLC announced that customers' payment card information was compromised by malware.

(n) On February 3, 2017, InterContinental Hotels Group announced that cash registers at more than 1,000 of its properties were infected with malware.

(o) On May 2, 2017, Sabre Hospitality Solutions revealed in its first quarterly report for 2017 filed with the SEC on Form 10-Q that it was "investigating an incident of unauthorized access to payment information" in its reservations systems. Like Marriott, Sabre's customers' credit card information and personal data were accessed by a hacker

who was able to infiltrate the company's reservation systems.

(p) In June 2017, Defendants were notified by independent cybersecurity researchers that hackers were able to access the email servers of Marriott's Computer Incident Response Team ("CIRT") due to an external analyst downloading a malware sample.

(q) In July 2017, several hotel chains, including Hard Rock Hotels & Casinos, Four Seasons Hotels and Resorts, Trump Hotels, Loews Hotels, Kimpton Hotels & Restaurants, RLH Corporation, and Club Quarter Hotels, among others, reported a data breach through a third-party reservations system provided by Sabre.

(r) In October 2017, Hyatt Hotels announced that it discovered unauthorized access to payment card information at 41 of its properties. This announcement followed Hyatt's earlier announcement in late 2015 that hackers had gained access to credit card systems at 250 properties.

(s) In August 2018, China-based Huazhu Hotels Group reportedly suffered a colossal data breach where the personal information of more than a hundred million hotel guests was stolen and sold on the dark web.

(t) On November 1, 2018, Radisson Hotel Group ("Radisson Hotel") announced a breach that impacted 10% of its rewards members in its rewards program database. Customers' names, addresses, email addresses, and in some cases, business contact information were all compromised as a result of the breach.

199. Significantly, between 2015 and 2017 alone, Starwood was affected by at least five different cybersecurity incidents of varying degrees of severity. Indeed, less than a week before the Company and Starwood signed the Merger agreement, on November 20, 2015, Starwood

disclosed that the POS systems at 54 of its hotels in North America had been infected by malware. After this latest Starwood data breach, it hired a PCI Forensic Investigator who determined that the data breach occurred because of violations of PCI DSS Requirements 1 and 8 (and additional PCI DSS requirements). Starwood continued to violate these requirements even after Marriott acquired it.

200. In addition to data breaches in the hospitality industry, the public, including Defendants, learned of the following cyber incidences at the time of each occurrence because it was publicly reported. Defendants also learned of these cyber-attacks at Board meetings. *See* Section VII.B.(3).

201. Defendants also knew or recklessly disregarded many other well-publicized data breaches involving other types of major corporations, including:

(a) Going back to 2013, through a series of data breaches more than three billion Yahoo! user accounts were compromised.

(b) In 2013 and 2014, and in separate incidents, hundreds of millions of Target and the Home Depot retail customers were victimized by hacks of payment card systems at those establishments.

(c) In 2015, Anthem, Inc., a health insurer, suffered a data breach that exposed personal information of nearly 80 million current and former plan members.

(d) Between May and July 2017, credit reporting agency Equifax suffered a data breach that affected nearly 150 million Americans, which was announced in September 2017. Notably, this shocking data breach was disclosed during Marriott's purported Integration and was tied to many of the same deficiencies that plagued Starwood's systems.

202. As outlined above, at a Board meeting on February 10, 2017, the Director Defendants learned that Starwood did not meet the standards of PCI DSS or meet PCI requirements. Additionally, the Director Defendants learned that Starwood did not utilize tokenization or point-to-point encryption. Defendant Hoffmeister knew this since he gave this report to the Director Defendants at this Board meeting. As a result of these PCI DSS violations, Hackers were able to directly communicate with Starwood's PCI-related systems and gain access to its cardholder data environment ("CDE") using single-factor authentication. After gaining access to those systems, Hackers were able to access unencrypted payment card numbers. Additionally, logging of remote access to systems and/or applications within the Starwood CDE was not configured. Because logging of remote access was not configured, Marriott lacked the ability to review any logs related to remote access to the Starwood CDE.

### F. The PFI Report Demonstrates That Defendants Misled The Market Regarding Their Due Diligence And Security Risks With The Starwood System

203. On May 6, 2019, a PFI Report was released which analyzed the Data Breach and determined there was unauthorized access to Starwood's guest reservation database. Additionally, the PFI Report identifies four PCI DSS requirements not met, and at least three "that likely [were] a contributing factor to the exposure, breadth of attack, and/or ease by which the attacker(s) gained access to the cardholder data environment." See Exhibit A-1 - PFI Report[15] at 106.

204. On September 19, 2019, John Reed Stark, president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm, and author of *The Cybersecurity Due Diligence Handbook*, published an article titled *Some Good News for the Cybersecurity Class*

[15] The public version of the PFI Report is attached hereto as Exhibit A-1. Plaintiffs also attach as Exhibit A-2 a legend explaining the various naming conventions utilized in the PFI Report. As detailed in Exhibit A-2, certain terms in the PFI Report have been replaced with generic identifiers, i.e., naming conventions.

*Action Bar*, where he states:

> Payment Card Industry Data Security Standards (PCI-DSS) is a set of requirements created to help protect the security of electronic payment card transactions that include personal identifying information (PII) of cardholders, and operates as an ***industry standard*** for security for organizations utilizing credit card information. PCI-DSS applies to all organizations that hold, process or pass credit card holder information and imposes requirements upon those entities for security management, policies, procedures, network architecture, software design and other critical measures that help to protect customer credit and debit card account data.
>
> The Payment Card Industry Security Standards Council (PCI SSC), an international organization founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. in 2006, develops and manages certain credit card industry standards, including the PCI-DSS. In addition to promulgating PCI-DSS, the PCI SSC has developed a set of industry rules governing responses to payment card data breaches. These rules, known collectively as the Payment Card Industry Forensic Investigator (PFI) program, were intended to replace the programs established by the individual card brands.
>
> ***Once a data security incident occurs… the [company] is contractually obligated to hire a specially certified PCI-approved forensic investigative firm (also known as a "PFI") from a small and exclusive list of card brand approved vendors (currently comprised of 22 companies).***
>
> ***The PFI team then performs a specified list of investigative work including writing a final report about the data security incident – the PFI Report*** — that is issued to both the [company] and the various credit card companies. The PFI Report then becomes the basis used by the card brand companies to calculate potential fines that will be levied against the acquiring banks. These fees are then passed along to the victim company in the form of indemnification. [Emphasis added].

205. On December 5, 2018, and after the Data Breach, Marriott retained Verizon to conduct a forensic investigation relating to the Data Breach. On December 12, 2018, Verizon started its investigation and authored a report based on this Data Breach titled "Starwood Hotel Resorts, LLC Final PFI Report", detailing its industry standard investigation and findings.

206. The PFI Report describes the poor state of Starwood's systems at the time of the Merger announcement, at the time of closing of the Merger, and throughout Marriott's use of the legacy Starwood guest reservation database. Further, and contrary to Defendants' statements

throughout the Relevant Period regarding Marriott's due diligence, the PFI Report demonstrates that Marriott failed to conduct meaningful due diligence on Starwood's compromised IT and data security systems, and/or failed to act on the findings of that due diligence by remediating the risks identified during the due diligence process. Regarding Starwood PCI DSS compliance, Defendants knew that Starwood was not compliant with PCI DSS requirements as of at least February 10, 2017, because they were notified of this at a Board meeting on that date. *See* Section VII.B.(3).

207. The PFI Report generally describes the Data Breach as follows: (1) an unknown threat actor(s) were able to remotely access a server within the Starwood CDE by exploiting known software vulnerabilities; (2) the Hacker(s) installed malware on that server and other servers which allowed the Hackers to capture the username and passwords for certain user and administrator accounts within the Starwood CDE; (3) the Hackers used the credentials from the user and administrator accounts to move through the Starwood CDE for the purposes of installing additional malware and compiling sensitive personal information; (4) the Hackers then staged that sensitive information on another server; (5) and after staging that sensitive information obtained from accessing the Starwood CDE, the Hackers then transferred that data to a server with internet connectivity before sending that sensitive data to a computer outside the Starwood CDE.

208. As stated in the PFI Report, Verizon performed analysis on 1,200 systems across 67 Starwood locations, and found conclusive evidence of the Data Breach. PFI Report at 16. The PFI Report shows that the Data Breach occurred because Starwood's system lacked sufficient data security. Specifically, Verizon identified four main causes of the Data Breach:

- Starwood's system allowed for insecure remote access making it easier to hack:
    - Certain administrator user groups were excluded from the requirement to

use multi-factor authentication to access the CDE;

- Starwood had no or insufficient firewall logging for its database access/query types:
    - Not all access/query logs were being aggregated to a centralized SIEM. Those logs not sent to a centralized SIEM were only stored on database servers for a short amount of time, and then eventually over written;
- Starwood lacked monitoring and logging of remote access:
    - There was no way to monitor who was accessing the systems because logging associated with remote access to Starwood's CDE was not configured; and
- Starwood stored payment account numbers on systems and in databases that were not designated for the storage of payment account numbers:
    - As a result, Starwood and Marriott were leaving sensitive data exposed.

PFI Report at 17-19; 31-32.

209. As stated in the PFI Report, the Data Breach began on or around July 28, 2014 when "an unknown threat actor gained access to the Starwood environment by installing malware on an external-facing webserver." PFI Report at 5. This window of intrusion, *i.e.* -- the time between the first confirmed date that an intruder entered the system until the date of containment, continued from that date until September 26, 2018. PFI Report at 24. However, Marriott's window of vulnerability, *i.e.* -- the period where a weakness in a system could be exploited by a threat, was from July 28, 2014 through December 21, 2018 – when the Data Breach was remediated. PFI Report at 24.

210. The PFI Report makes clear that Starwood was storing large quantities of payment card information and for an unreasonably long period of time, going back to 2002, in violation of the FTC's guidance on data security. PFI Report at 25.

211. The malware found on Marriott's system included (1) web shells; (2) Remote Access Trojans (RATs); (3) password stealers; (4) reconnaissance tools/scripts; (5) network/connectivity tools; (6) file archiving utilities; and (7) Random Access Memory (RAM)-scraper malware. PFI Report at 5. *See* Acronyms and Definitions at Exhibit B attached hereto for an explanation of each of these types of malware. By way of example to illustrate the extent of this malicious intrusion, the PFIs found RAM-scraper malware on 480 systems spread out across 58 Starwood locations. PFI Report at 69. Eight of those systems related to payment card processing functions. PFI Report at 71. Of the 54 locations, 13 were affected by the Starwood November 20, 2015 POS breach were again infected by RAM-scraper malware. Yet, at this time, the breaches occurred directly under Defendants' watch, even though Defendants knew that the same type of malware had impacted those same locations just a year earlier.

212. The PFIs determined that the Hackers, using this malware, performed unauthorized queries against the Starwood guest reservation database, shortly thereafter exported the main guest reservation database table and placed it into a compressed and password protected (rar) archive, and then, using a transfer tool, moved this compressed file to an external IP address.

213. The Starwood guest reservation database table discussed above contained more than 9 million encrypted payment card numbers. This guest reservation database table included each customer's (1) name; (2) address; (3) telephone number; (4) encrypted payment card number; and (5) payment card expiration date. PFI Report at 5. The PFIs also identified 7,243 potential unencrypted payment card numbers in other fields in two guest-reservation database tables that were exported and exfiltrated, and another 236,504 potential unencrypted payment card numbers inadvertently stored throughout 40 Starwood systems. PFI Report at 73.

214. The PFI Report also discusses (pp. 106-109) four PCI DSS requirements violated

by Starwood and Marriott: (1) Requirement 1.2 stipulates that firewall and router configurations must restrict all traffic, inbound and outbound, from untrusted networks and hosts; (2) Requirement 3.4 stipulates that cardholder data be rendered unreadable anywhere it is stored, including digital media, backup media, in logs, and data received from or stored by wireless networks; (3) Requirement 8.3 stipulates that entities must secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication; and (4) Requirement 10.2 stipulates that entities must implement automated audit trails for tracking individual user access to cardholder data and all actions taken by any individual with root or administrative privileges.

215. The PFI Report discusses Marriott's containment plan relating to the Data Breach at pages 98-99 and lists 27 containment actions completed between September 8, 2018 and January 11, 2019. These completed actions included the decommissioning of the entire Starwood CDE environment.

216. Importantly, the PFI Report notes containment actions not completed by Marriott as of the date of the report, which are: (1) "[l]everage EDR ["endpoint detection and response"] and other security tools to perform searches for known IOC's ["indicators of compromise"] (ongoing detection/protection)"; (2) "[i]mplement additional enhanced monitoring for log sources being aggregated to a SIEM"; (3) "[i]mplement additional log sources being aggregated to the SIEM"; and (4) "[d]elete files containing PANs ["primary account numbers"] from inadvertent storage on various systems[.]" PFI Report at 100.

217. The PFI Report also includes, in the order of priority, recommendations to reduce the risk of another data breach: (1) "Search the PCI Environment for Track Data / PANs"; (2) "Restrict and Monitor Remote Access"; (3) "Implement a Binary Whitelist"; and (4) "Clear

Pagefile Upon System Shutdown ." PFI Report at 101-102.

218. The ongoing containment actions and recommendations to reduce the risk of another data breach are particularly important in light of Marriott's most recent data breach in January 2020, impacting approximately 5.2 million guests.

### G. The Company's Internal Documents Demonstrates That Defendants Misled The Market Regarding Their Security Risks With The Starwood System

219. Marriott's own documents shows that: (1) Defendants made false statements to the market; and (2) did so either knowingly or with severe recklessness.

220. At a meeting of the Marriott Board on August 7, 2014, Defendant Sorenson and other board members discussed "some recent publicized [data breach] incidents," including the Target breach discussed in Section VII.E., and received a presentation titled "Security Overview" detailing recent cybersecurity incidents at other companies. Nevertheless, Defendant Sorenson and the rest of the Board failed to retain the services of an outside analyst or consultant to audit any cybersecurity risks Starwood brought to the Merger.

221. Only days after the Merger was announced, Starwood disclosed that the POS systems at some of its hotels in North America had been infected with RAM-scraper malware and that the software had been infected from November 2014 to October 2015 (the 2015 Starwood Data Breach). The malware allowed cybercriminals to access the payment card data of Starwood customers. Notwithstanding this significant development, Marriott's Board did not act. The Board did not order a more detailed and focused review of Starwood's IT operations, and merger negotiations continued without concern.

222. While Defendant Sorenson and the rest of the Board, including the Audit Committee Defendants, failed to act to ascertain the depth of the cybersecurity issues publicly

identified by Starwood, there is no question that the Board understood the threat facing Marriott stemming from Starwood's disclosed breach and Starwood's related cybersecurity deficiencies at the time it claimed to be conducting due diligence on Starwood.

223. At the Company's Board meeting on February 12, 2016, approximately seven months prior to the closing of the Merger, Defendant Oberg, the Company's CFO, gave a presentation on risks facing Marriott to the Board, which included Defendant Sorenson and the Audit Committee Defendants. Defendant Oberg's presentation ranked the top risks facing Marriott in 2016, and included a slide titled "Overall Company Risk Ranking," which showed that the Board itself ranked cybersecurity as the number one risk facing Marriott in 2016. "Information Protection" also made the list of risks. Marriott's executive management team provided its own assessment, also listing cybersecurity high on its list of threats facing the Company. One slide presented to Defendant Sorenson and the rest of the Board, including the Audit Committee Defendants, summarized the Board and management's understanding of the Company's cybersecurity risk succinctly.

224. At the same Board meeting, Defendant Sorenson was provided with the results of a survey of 270 of Marriott's top executives. One slide in that presentation showed that 59% of these executives considered cybersecurity as a "High/Substantial" risk. A second slide showed that 38% of the executives believed that Marriott's mitigation plans to address the cybersecurity risk should be "significantly enhanced" or "enhanced," and another 38% responded that "certain areas could be enhanced to more fully address the risk."

225. While the Board and the Company's management acknowledged the threat of cybersecurity to the Company's future, minutes from various Board meetings held while Marriott was supposed to be conducting due diligence into Starwood's cybersecurity revealed not a single

mention of Starwood's cybersecurity or data controls. Rather, these minutes indicate that Marriott's Board received information on the "related costs of establishing and continually evolving [cybersecurity] infrastructure to prevent and manage them" but not information regarding Starwood's existing controls and vital data. It was not until after Merger actually closed that the Board was brought up to speed on Starwood's IT systems. Marriott's Board recommended the Merger with Starwood in November 2015, and the Merger closed on September 23, 2016, notwithstanding the failures in the due diligence Marriott conducted of Starwood's cybersecurity systems, and failure to discover how vulnerable Starwood's systems, and specifically the guest reservation database, were.

226. Marriott's management made the decision to continue using Starwood's old reservations systems post-Merger, knowing that they had been breached at least once, recently, and knowing that Starwood's cybersecurity efforts did not comply with industry standards or the applicable laws and regulations. Minutes from a December 3, 2018, presentation by Marriott's management to the Board, show that Marriott made what management referred to as "security decisions" at the time of the Merger in deciding not to invest in Starwood's systems because they intended to operate the legacy Starwood guest reservation database for a short time. However, Marriott did not decommission the legacy Starwood guest reservation database until more than two years after the Merger closed and approximately three months after Marriott was first alerted to the Data Breach. *See* Section VII.F.

227. The Board and its committees, including the Audit Committee, met on February 8, 2017. Members of the Audit Committee were informed by its consultant, E&Y, that "[w]hile cybersecurity has historically been a topic of discussion in board rooms, the increase in the volume and severity of attacks, coupled with the increased scrutiny by regulators, has significantly elevated

its importance." It was the Audit Committee that was "now expected to have an understanding of the business implications of cyber risks" and that "cybersecurity has emerged to prominence as a massive risk area for the hospitality industry." E&Y also informed the Audit Committee that they were expected to have an understanding of the appropriateness of the Company's cybersecurity risk disclosures required by the SEC. Marriott's own internal audit department rated Marriott as "Needs Improvement" in cybersecurity. And Marriott's chief audit executive ("CAE"), Keri Day, stated that Marriott's "incident response plan is not up to date and does not include detailed playbooks/procedures for responding to highly probabl[e] incidents and protocols for invoking Marriott's broader Crisis Management Plan."

228. Notwithstanding the directive from E&Y in 2017 that the Audit Committee, specifically, should be tasked with overseeing cybersecurity risk, the Company did not move responsibility for cybersecurity risk oversight from the entire Board to the Audit Committee until January 2019.

229. Defendant Sorenson and the rest of the Board, including the Audit Committee Defendants, were also reminded at the February 10, 2017, Board meeting that cybersecurity remained a top-level risk for the Company. According to Defendant Oberg's presentation, the Board ranked cybersecurity as the second biggest risk facing Marriott in 2017, and that the hospitality industry was "a target for cyber criminals," and "continuous efforts to identity and mitigate risks is required."

230. The Board also received a presentation titled "Marriott Cybersecurity Report," which showed that 30 hospitality companies experienced data breaches in 2015, and another 21 did in 2016. This presentation also included a slide that showed that, specifically, HEI, Mandarin, Hilton, and Starwood had all experienced breaches in the past three years.

231. At the February 10, 2017, Board meeting, Defendant Sorenson and the Audit Committee Defendants, along with the rest of the Board, learned much more about the lack of cybersecurity controls involving Starwood's legacy databases, databases still in use after the merger. PwC was brought in to assess Starwood's systems, and created the "Starwood Security Program Assessment." After Defendant Hoffmeister presented PwC's "early observations" from this assessment, including [redacted], a presentation given to the Board explained that Starwood's "[b]rand standards did not mandate PCI compliance, tokenization, or point-to-point encryption." Marriott's due diligence process should have uncovered Starwood's lack of PCI DSS compliance, as seeking to be compliant with relevant laws and regulations is a part of any standard due diligence process. PwC's assessment also reported that Starwood's "[d]ecentralized technology management model created a different risk profile than Marriott's centralized approach" which "[a]llowed for greater opportunity for deviation from the expected published standard, and led to an unusually high number of associates with elevated access to systems." Defendant Sorenson and the rest of the Board, including the Audit Committee Defendants, would have known all of this sooner had a proper due diligence investigation been conducted, and if the results had been reported to the Board, or the Board knew of and were severely reckless in disregarding these risks. Additionally, as Defendant Oberg noted, the Board recognized that cybersecurity was among the top risks facing Marriott. If Defendants did not know before the February 2017 Board meeting, they definitely knew afterwards that Starwood was not PCI DSS compliant. Notably, Marriott protected its client data using tokenization.

232. PwC provided Marriott's Board, including Sorenson, with four "key recommendations" including: 1) Update Starwood brand standards to mandate PCI and set cybersecurity expectations; 2) Strengthen the security of systems that manage user accounts and

passwords; 3) Tightly control user accounts that have elevated (administrator level) privileges to critical systems; and 4) Continue to analyze Starwood's technical environment to identify items exceeding Marriott's risk appetite.

233. For a full year following the February 2017 Board meeting, based on Board minutes, the Board did not reconsider or address the known, identified deficiencies associated with Starwood's databases, and customer reservations continued to be made using Starwood's antiquated, non-compliant guest reservation system. At the February 9, 2018, meeting of the Board, Defendant Sorenson and the Audit Committee Defendants, were informed that for the past year, Marriott had elected to simply "[i]mplement[] patching" to fix issues related to Starwood's unsafe databases, and that the transition and "[m]igration of Starwood systems to the Marriott established technology standards for PCs, Laptops and other end user devices" would not be completed until September, 2019, three years after the merger closed. Defendant Sorenson and the other Board Members also heard from Defendant Oberg at this meeting, when she reminded them that "both management and the Board viewed … cybersecurity among the top risks facing the Company."

234. The bad news kept coming. The Board, including Defendant Sorenson and the Audit Committee Defendants, was informed on August 9, 2018, that Marriott found "[m]alware on a legacy-Starwood server used by the Marriott Law Department" back in January 2018. At the same meeting, Defendant Sorenson and the Audit Committee Defendants also learned about additional security events or incidents. Starwood's vulnerable guest reservation database remained in use, even after the Board acknowledged at the February 9, 2018, Board meeting that cybersecurity remained a "Top Five" risk facing the Company. However, despite the acknowledgement of the risk cybersecurity posed, Marriott's mitigation efforts did not include any

efforts to update the legacy Starwood systems.

### H. Experts' Reaction To The Data Breach

235. Reactions to the Data Breach from cybersecurity experts reveal its severity and that experts were surprised that Marriott did not identify the data breach during its due diligence.

236. For example, Ollie Whitehouse, Global Chief Technology Officer at IT security company NCC Group, stated that Marriott Hotels should have identified this breach through their cyber due diligence of Starwood in 2016 when it acquired the company. As result of buying a breach they will face a number of challenges at a board level around the levels of governance and diligence within the business. Had it performed a detailed compromise assessment as part of its due diligence activity, the organization's board would have been informed of the breach and been able to make a decision based on risk or put other warranties in place.

237. Joseph Carson, Chief Security Scientist at security company Thycotic, stated that: "What is shocking about this data breach is that the cybercriminals potentially got away with both the encrypted data as well as the methods to decrypt the data which appears that Marriott have not practiced adequate cybersecurity protection for their customers[‘] personal and sensitive information."

238. Satya Gupta, Global Chief Technology Officer and Co-Founder of cybersecurity company Virsec, stated that: "What's most disturbing about this attack is the enormous dwell time inside Starwood's systems. The attackers apparently had unauthorized access since 2014—a massive window of opportunity to explore internal servers, escalate privileges, move laterally to other systems, and plot a careful exfiltration strategy before being discovered. All organizations should assume that the next threat is already inside their networks and won't be caught by conventional perimeter security. We need much more careful scrutiny of what critical applications

are actually doing to spot signs of internal corruption. We must reduce dwell time from years to seconds."

239. Tom van de Wiele, a security consultant at cybersecurity and privacy company FSecure, stated that: "The most disappointing part of this hack is the fact that the amount of data stolen is one of the bigger ones of the last few years and further made worse by the fact that the compromise had been going on for at least four years according to several online publications. This indicates that as far as security monitoring and being able to respond in a timely and adequate fashion, Marriott had severe challenges being able to live up to its mission statement of keeping customer data safe."

240. On March 7, 2019, the U.S. Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations held a hearing on "Examining Private Sector Data Breaches" during which Democratic Sen. Jacky Rosen (Nev.), who previously worked in IT, expressed surprise that Marriott had "no method of auditing the data coming across" following its acquisition of Starwood

## VIII. THE COMPANY'S AUDIT COMMITTEE

241. During the Relevant Period, Marriott's Audit Committee (the "Audit Committee") met at least seventeen (17) times. At the start of the Relevant Period, the Audit Committee had three members: Defendants Bush, Henderson (also the Chair of the Audit Committee), and Kellner. On September 23, 2016, when the Merger closed, the Audit Committee expanded to five (5) members, including a former member of Starwood's board of directors. Defendants Bush and Henderson remained on the Audit Committee, with Henderson retaining his position as Chair, and were joined by Defendants Muñoz and Lewis—the former member of Starwood's board.

242. During 2015, 2016, and 2017, the Audit Committee's responsibilities included: (1)

overseeing the Company's accounting, reporting, and financial practices, including the integrity of the financial statements; (2) overseeing the Company's internal control environment and compliance with legal and regulatory requirements; (3) appointing, retaining, overseeing, and determining the compensation for and terms of the agreement with the Company's independent auditor; and (4) overseeing the Company's internal audit function and the internal auditor.

243. At the start of 2018, in addition to the responsibilities just listed, the Audit Committee was also tasked with "[a]ssisting the Board in overseeing and monitoring the Company's information security and data privacy practices." According to Marriott's Annual Proxies in each of 2015, 2016, 2017, and 2018: "There is unrestricted access between the Audit Committee and the independent auditor and internal auditors." In the Audit Committee Charter during the Relevant Period, the Audit Committee was required to "periodically review and discuss the Company's business and financial risk management and risk assessment policies and procedures with senior management, the Independent Auditor, and the Chief Audit Executive."

244. The Audit Committee Defendants signed the Company's Form 10-Ks during the Relevant Period. Additionally, Defendants Bush, Henderson, Kellner, and Muñoz signed the Company's Recommendation Statement for the Merger.

## IX. FALSE AND MISLEADING STATEMENTS AND OMISSIONS[16]

### A. Letter To The Company Associates Regarding The Merger

245. On November 16, 2015, the Company filed a prospectus containing a letter from Defendant Sorenson to Company associates discussing the Merger and what the Company's associates should expect. Defendant Sorenson stated:

> This union will also generate tremendous growth: growing value for shareholders, growing choices and benefits for consumers, growing economic advantages for our

[16] The statements that are ***bolded and italicized*** in this section are statements alleged to be false or misleading.

owners and franchisees, and growing opportunities for associates.

> ***This integration will require a significant amount of work, but while the scale is much larger, we have successfully completed integrations before. We have always emerged stronger, and better positioned, to compete in a rapidly changing marketplace.***

246. Defendant Sorenson also stated: "***The team will guide the Starwood integration and ensure that it succeeds with minimal disruption to our business.***"

247. Defendant Sorenson further stated:

> Delighting our guests is the priority, ***and we don't anticipate the integration having an impact at the hotel level worldwide.*** There will be some support areas where we overlap and we'll address those in time as we look to more efficiently run our combined organization.

248. These statements and omissions regarding the state of the Integration and the Company's prior integration experience were false and misleading when made because at the time these statements were made, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have revealed these glaring deficiencies, yet Defendants knowingly, or with severe recklessness, failed to share this crucial information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

249. Further, the statements and omissions: (1) gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants caused the Company to fail to secure Starwood's systems, despite knowledge of cybersecurity risks; and (2) gave the market/investors the false sense that the Company's prior acquisition experience was relevant to the Merger due diligence and Integration processes, and was in fact guiding those processes. In addition, as detailed in the Board minutes pleaded in Section VII.G., Defendants were well aware of the risk that cybersecurity posed to the Company, however, Defendants ignored multiple red flags that should have caused them to discover the Data Breach, including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E); and (3) other significant data breaches in other industries, as detailed in Section VII.E.

**B. Registration Statements**

250. On December 22, 2015, the Company filed its Form S-4 Registration Statement (the "Registration Statement") related to the Merger. The Registration Statement was signed by Defendants Sorenson and Bauduin, and the Audit Committee Defendants.

251. On January 27, 2016, the Company filed the First Amendment to the Registration Statement (the "First Amended Registration Statement"), which was signed by Defendants Sorenson and Oberg.

252. On February 16, 2016, the Company filed the Second Amendment to the Registration Statement (the "Second Amended Registration Statement"), which was signed by Defendant Sorenson.

253. On February 17, 2016, the Company filed a prospectus pursuant to SEC Rule

424(b)(3) related to the Merger (the "First Prospectus"). The First Prospectus was signed by Defendant Sorenson.

254. The Registration Statement, First Amended Registration Statement, Second Amended Registration Statement, and the First Prospectus stated that the Board, in arriving at its decision to recommend the Merger, "***consulted with Marriott's senior management, legal advisors, financial advisors, and other advisors," and later stated that the Board "reviewed a significant amount of information***." Additionally, those documents informed the market that "***both Marriott's and Starwood's strong track records in merger integration***" supported voting in favor of the Merger.

255. Further, in the Registration Statement, First Amended Registration Statement, Second Amended Registration Statement, and First Prospectus, when listing the strategic and financial benefits of the Merger, the documents stated:

> All 11 of Marriott's current directors will continue to serve on Marriott's Board with the expected addition of three members of Starwood's current board, ensuring continuity of Marriott's Board and the addition of directors with a deep knowledge of Starwood, enhancing the Marriott Board's understanding of the integration process.
>
> * * *
>
> ***Given Marriott's Board's knowledge of Marriott's business, operations, financial condition, earnings and prospects and Marriott's Board's knowledge of Starwood's business, operations, financial condition, earnings and prospects, taking into account Starwood's publicly filed information and the results of Marriott's due diligence review of Starwood, the prospects for the combined company are favorable.***

256. These statements and omissions regarding the Company's preparedness, and the state of the Integration up to that point were false and misleading when made because at the time these statements were made, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched;

(2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

257. Further, the statements and omissions: (1) gave the market/investors a false impression that the Company had undertaken sufficient due diligence in accordance with relevant requirements, standards, and best practices detailed above; (2) gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks; and (3) gave the market/investors the false sense that the Company's prior acquisition experience was relevant to the Merger due diligence and Integration processes, and was in fact guiding those processes. In addition, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, including ranking cybersecurity as a top risk facing the Company, however, the Director Defendants ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, now including the RAM-scraper breach announced on

November 20, 2015, and as detailed in Sections VII.A., B.(4),E., and F.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, now including the FTC's settlement with Wyndham hotels announced on December 9, 2015, and as detailed in Section VII.D.(2) and E.; and (3) other significant data breaches in other industries, as detailed in Section VII.E.

### C. Fourth Quarter 2015 Earnings Call

258. On February 18, 2016, the Company held a conference call to discuss fourth quarter 2015 ("Q4 2015") earnings, the Merger, and other topics. An analyst asked Defendant Sorenson about avoiding pitfalls in an acquisition and Defendant Sorenson responded:

> Analyst
>
> So, if you guys could talk about the challenges that you face integrating the two companies and their systems. We are getting several questions about, going back to the Ryman acquisition, how -- I guess the question really is, what are you doing to be as thorough as you can so that you avoid some of the pitfalls?
>
> Defendant Sorenson
>
> Yes, it is a good question. I think we are hopefully learning from the experiences we have had in the past few years. You can, to some extent, look at the Gaylord acquisition and the Protea and Delta acquisitions as warm-up acts for this, I suppose, and hopefully we're getting better at it.
>
> Now at the same time, obviously, Starwood is a much bigger deal than any of those were, which presents some positive differences and then some greater challenges. I think on the positive side Starwood is hopefully less distracted by the process of the sale of the company, and you have got a big, talented group of folks over there running 350,000 rooms or so. But I know the Starwood team, with our encouragement, is very much focused on continuing to drive sales and to drive the development engine, and we have taken steps to try and put our arms around those teams of folks so that they are as little distracted by this as possible
>
> I think some of the other deals we did early, it was that sales engine which looked like it got distracted during a sales process and to some extent between the negotiator -- the signing of a deal and the closing of a deal.
>
> ***And we are doing everything we can to plan for integration of systems and integration of business units between now and when we close so that we can***

***implement those as quickly as possible. And we're optimistic at this point that this will go well.***

259. These statements and omissions regarding the Integration planning up to that point were false and misleading when made because at the time Defendant Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendant Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

260. Further, the statements and omissions gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendant Sorenson failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Sections VII.B.(3) and E.; (2)

significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; and (3) other significant data breaches in other industries, as detailed in Section VII.E..

**D. The 2015 Form 10-K**

261. On February 18, 2016, the Company to file the Company's Form 10-K for year ending 2015 ("2015 Form 10-K"). The 2015 Form 10-K was signed by Defendants Sorenson, Oberg, and Bauduin, the Audit Committee Defendants, and Defendants JW Marriott, Harrison, Lee, Reinemund, and Schwab and made representations regarding the security of customer data, the Company's operations, and the Merger.

262. In the 2015 Form 10-K reported:

> Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***the integrity and protection of customer, employee, and company data is critical to us*** as we use such data for business decisions and to maintain operational efficiency.

263. These statements and omissions concerning the "***integrity and protection***" of data being "***critical***" to the Company were false and misleading when made for the reasons detailed in ¶¶ 259-260.

264. The 2015 Form 10-K described **potential** risks the Company **might** face as a result of the Merger:

> The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in*** the loss of valuable employees, ***the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies*** and compensation arrangements, ***any of***

> ***which could adversely affect the combined company's ability to achieve the benefits we anticipate***. The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, and ***the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes. The combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies. The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect. If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.***

265. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. In addition, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

266. The 2015 Form 10-K described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> * * *
>
> ***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit***

***large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

* * *

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.

* * *

***Any disruption in the functioning of our reservation system, such as in connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly***

> ***with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

267. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. In addition, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

268. Attached to the Company's 2015 Form 10-K were certifications[17] signed by Defendants Sorenson and Oberg that stated:

> ***I have reviewed this annual report on Form 10-K of Marriott International, Inc.;***
>
> ***Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report. . . .***

269. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the 2015 Form 10-K, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them

[17] Under the Sarbanes-Oxley Act of 2002 ("SOX"), the CEO and CFO of publicly traded companies are required to sign certifications attesting to the fact that they have reviewed the company's quarterly SEC filings for false statements, and that they have reviewed the company's internal controls and processes to ensure the accuracy of the company's financial statements (the "SOX Certifications").

at the time concerning the risks that existed to the customer data. In addition, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

**E. March 21, 2016 Conference Call**

270. On March 21, 2016, the Company held a conference call to discuss the Amended Merger Agreement. Defendant Oberg stated:

> ***After we've had extensive due diligence and spending a lot of time with the Starwood team and joint integration planning,*** we increased our targeted annual G&A cost synergies to $250 million, up from $200 million. And excluding any benefit from even more incremental cost savings beyond the $250 million and additional revenue synergies which we're confident we will provide, we expect adjusted EPS to be roughly neutral in 2017 and 2018.

271. In discussing the Company's due diligence, Defendant Sorenson stated:

> ***In the further diligence we have completed in last five months, we have become even more convinced of the tremendous opportunity presented by this merger. That confidence is reflected in our higher offer. We now believe there are more cost synergies than we estimated in November.***

272. Defendant Sorenson also stated:

> We've talk a little bit about cost synergies. This is now on page 10 for those of you who are following along. ***We have been working intensely since we announced this deal in November to prepare for integration and of course, to understand each other's organizations and structures and start to think about how to meld those into one organization.***

273. On March 21, 2016, Defendant Sorenson also posted a statement to LinkedIn:

> Since we announced the merger in November 2015, our integration teams have met on average multiple times a week across disciplines. ***As a result of our extensive due diligence and joint integration planning, we are now even more confident in the potential of cost savings of this transaction***.

274. These statements and omissions concerning the Company's due diligence, including "***extensive due diligence and joint integration planning***," and Integration planning up to that point were false and misleading when made because at the time Defendant Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems

were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

275. Further, the statements and omissions: (1) gave the market/investors a false impression that the Company had undertaken sufficient due diligence in accordance with relevant requirements, standards, and best practices detailed above; and (2) gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. In addition, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Sections VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other

industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of the GDPR. *See* Section VII.H.(4).

**F. March 21, 2016 Prospectus**

276. On March 21, 2016, the Company filed a Prospectus containing an updated letter to the Company's associates explaining the Company's strategy regarding the Merger. Defendant Sorenson stated:

> Beyond the math, the strategic story hasn't changed. The simple fact remains that the combination of Marriott and Starwood will create a premier lodging company that will offer broader choice for guests, greater benefits for owners and franchisees, more opportunities for associates and increased value for shareholders of both companies. ***Over the course of the last few months we've had an opportunity to learn even more about Starwood through our integration process and we believe that the benefits of combining both companies are even more compelling than our original expectations.***

277. These statements and omissions regarding the progress of the Integration up to that point, was false and misleading when made because at the time Defendant Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendant Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest

reservation database was already compromised by the Data Breach.

278. Further, the statements and omissions gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E; (3) other significant data breaches in other industries, as detailed in Section VII.E; and (4) the passage and imminent enforcement of the GDPR. *See* Section VII.H.(4).

**G. <u>The Form 8-K, dated March 21, 2016</u>**

279. On March 21, 2016, the Company filed an 8-K. It was in the press release attached to the Form 8-K that Defendant Sorenson:

> ***As a result of extensive due diligence and joint integration planning, Marriott is confident it can achieve $250 million in annual cost synergies within two years after closing, up from $200 million estimated in November 2015 when announcing the original merger agreement.***
>
> * * *
>
> . . . ***"After five months of extensive due diligence and joint integration planning with Starwood, including a careful analysis of the brand architecture and future development prospects, we are even more excited about the power of the combined companies and the upside growth opportunities."***

280. This statement and/or omission regarding the Company's "***extensive due diligence and joint integration planning***" up to that point was false and misleading when made for the reasons detailed in ¶¶ 259-260.

**H. The Company Press Release In Support Of The Merger**

281. On March 31, 2016, the Company issued a press release regarding the upcoming Starwood shareholder vote. Defendant Sorenson stated:

> We are focused on maximizing shareholder value and from the beginning of this process we have been steadfast in our belief that a combination with Starwood will offer the highest value to all shareholders. Together, we can provide opportunities for significant equity upside and great long-term value driven by a larger global footprint, wider choice of brands for consumers, substantial synergies, and improved economics to owners and franchisees leading to accelerated global growth and continued strong returns. ***Our integration teams have been diligent in their work over the last few weeks and are more committed than ever to a timely and smooth transition.***

282. These statements and omissions regarding Marriott's "***diligent***" Integration work up to that point were false and misleading when made for the reasons detailed in ¶¶ 259-260.

**I. Marriott And Starwood M&A Conference Call**

283. On April 1, 2016, the Company held a conference call to discuss the Merger. Defendant Sorenson stated:

> Analyst
>
> Good morning, everyone. A quick question on cost synergies. Just wondering if you can provide a little more elaboration on -- the previous estimate was $200 million, it went to $250 million, that is. What was included in the incremental $50 million, and is there any reason to believe that with more information there could be more to come on that front?
>
> Defendant Sorenson
>
> So Tom thought we could do $250 million from the moment we announced a deal. And he knows the cost structure at Starwood, obviously dramatically better than we do. And I guess in a way we just were acknowledging that he was right. For us, we want to take it a step at a time and we hadn't, when we announced the deal, really done any organizational diligence, if you will. ***We've done financial diligence and tried to understand the assets and the balance sheet and those sorts of things.***
>
> ***But in the four months we've had following, we've had -- I think one of our team, the Starwood integration [lead] counted 150-ish meetings between Marriott and Starwood people in various disciplines or various regions around the world,***

> ***where they are getting to know each other, where they are getting to know the organizations, where they are starting to think about what the combined organization looks like from a staffing level going forward.*** And all of that has given us greater confidence that the $250 million number is achievable. We don't have another number to hang out for you as further upside from that.

284. These statements and omissions regarding the progress of the Company's due diligence and Integration planning up to that point were false and misleading when made for the reasons detailed in ¶¶ 259-260.

**J. Form 8-K, dated April 27, 2016**

285. On April 27, 2016, the Company filed a Form 8-K signed by Defendant Bauduin that included a press release. Defendant Sorenson stated:

> ***Our planned acquisition of Starwood Hotels & Resorts is on track.*** Shareholders of both companies overwhelmingly approved proposals relating to the merger and we continue to look forward to a mid-2016 closing. ***Toward that end, integration teams from both companies have been working over the last several months to ensure a smooth transition.*** We look forward to creating the largest lodging company in the world.

286. These statements and omissions concerning the state of the Integration, including that it was currently "***on track***," up to that point were false and misleading when made because at the time Defendants Bauduin and Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due

diligence process would have easily revealed these glaring deficiencies, yet Defendants Bauduin and Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

287. Further, the statements and omissions gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of the GDPR. *See* Section VII.H.(4).

### K. First Quarter 2016 Form 10-Q

288. On April 28, 2016, the Company filed its first quarter 2016 Form 10-Q ("Q1 2016 Form 10-Q", which was signed by Defendant Bauduin. The Q1 2016 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could***

> ***result in*** the loss of valuable employees, ***the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies*** and compensation arrangements, ***any of which could adversely affect the combined company's ability to achieve the benefits we anticipate.*** The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, and ***the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes. The combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies. The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect. If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.***

289. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendant Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. Additionally, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

290. The Q1 2016 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***

* * *

***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.

* * *

***Any disruption in the functioning of our reservation system, such as in***

> ***connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

291. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg, and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. Additionally, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

292. Attached to the Company's Q1 2016 Form 10-Q were identical SOX Certifications signed by Defendants Sorenson and Oberg that stated:

> ***I have reviewed this quarterly report on Form 10-Q of Marriott International, Inc.;***
>
> ***Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report. . . .***

293. These statements were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q1 2016 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time

concerning the risks that existed to the customer data. In addition, these statements were false and misleading when made for the reasons detailed in ¶¶ 259-260.

**L. Second Quarter 2016 Earnings Call**

294. On July 28, 2016, the Company held a conference call to discuss the second quarter 2016 ("Q2 2016") earnings, the Merger and Integration. Defendant Sorenson stated:

> I would also like to say that I have never been more proud of Marriott associates. This team has done a lot of transactions over the last five years from the spinoff of Marriott Vacations Worldwide in 2011 to the more recent acquisitions of AC Hotels, Gaylord, Protea and Delta. With each of these transactions, Marriott associates worked hard to first execute the transaction and then capture the strategic value of the deal all while growing and managing our existing business.
>
> The Starwood transaction should be completed in the coming weeks bringing these terrific teams together. ***Both the Marriott and Starwood teams have done exhaustive planning to get ready*** and we are excited by our prospects. While we will see a lot of progress in the near-term, we expect that full integration will be a two-year project.

295. These statements and omissions concerning the state of the Company's "***exhaustive***" Integration planning up to that point were false and misleading when made because at the time Defendant Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendant Sorenson

knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

296. Further, the statements and omissions gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks, which Defendants now knew included the fact that Starwood did not have visibility into its own out-of-date operating systems and/or malware on Starwood's systems, and that Starwood did not use point-to-point encryption or tokenization. In addition, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E; and (4) the passage and imminent enforcement of the GDPR. *See* Section VII.H.(4).

**M. Second Quarter 2016 Form 10-Q**

297. On July 28, 2016, the Company filed its second quarter 2016 Form 10-Q ("Q2 2016 Form 10-Q"), which was signed by Defendant Bauduin. The Q2 2016 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> The combined company may not be able to integrate successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a***

> ***number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in*** the loss of valuable employees, ***the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies*** and compensation arrangements, ***any of which could adversely affect the combined company's ability to achieve the benefits we anticipate.*** The combined company's resulting portfolio of approximately 30 brands could be challenging for us to maintain and grow, ***and the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate***. ***The combined company's results of operations could also be adversely affected by any issues attributable to either company's operations that arise or are based on events or actions that occur before the Starwood Combination closes. The combined company may also have difficulty addressing possible differences in corporate cultures and management philosophies. The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect. If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results and prospects could suffer.***

298. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

299. The Q2 2016 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if***

***we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***

* * *

***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches.

* * *

> ***Any disruption in the functioning of our reservation system, such as in connection with the Starwood Combination, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel web sites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking following consummation of the Starwood Combination. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

300. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg, and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

301. Attached to Marriott's Q2 2016 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

302. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q2 2016 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

**N. Marriott's Privacy Statement**

303. On September 23, 2016, the Company provided the market with a Global Privacy Statement through the Company's website, www.marriott.com. In the Global Privacy Statement, the Company provided the public with its policies and procedures for using, collecting, and storing the data the Company collects from its customers.

Security

> ***We seek to use reasonable organizational, technical and administrative measures to protect Personal Information within our organization.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section below.

304. These statements and omissions concerning the Company's data protection measures were false and misleading when made because at the time Defendants made these statements, Starwood's IT systems, now owned by the Company, were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

305. Further, the statements and omissions: (1) gave investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; and (2) gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. In addition, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of the GDPR. *See* Section VII.H.(4).

**O. Form 8-K, dated November 7, 2016**

306. On November 7, 2016, the Company filed an 8-K signed by Defendant Bauduin. Defendant Sorenson stated in the press release attached to this Form 8-K:

> We were thrilled to close the acquisition of Starwood in late September. We are enthusiastically engaged in welcoming Starwood's associates around the world into the Marriott family and ***are working diligently on integrating the companies*** and realizing revenue and cost synergies as quickly as possible.

307. These statements and omissions that Marriott was, at that point, "***working diligently***" on the Integration were false and misleading when made for the reasons detailed in ¶¶ 259-260.

**P. Third Quarter 2016 Form 10-Q**

308. On November 9, 2016, the Company filed its third quarter 2016 Form 10-Q ("Q3 2016 Form 10-Q"), which was signed by Defendant Bauduin. The Q3 2016 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We entered into the Merger Agreement with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner.***
>
> ***The integration process could also take longer than we anticipate and could result in*** the loss of valuable employees, ***the disruption of each company's ongoing businesses, processes and systems or inconsistencies in standards, controls, procedures, practices, policies*** and compensation arrangements, ***any of which could adversely affect the combined company's ability to achieve the benefits we anticipate. Our resulting portfolio of approximately 30 brands may be challenging for us to maintain and grow, and the harmonization of our different reservations and other systems and business practices could be more difficult, disruptive, and time consuming than we anticipate. We may also have difficulty addressing possible differences in corporate cultures and management philosophies.*** We may incur unanticipated costs in the integration of the businesses of Starwood. Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.
>
> ***The integration process is subject to a number of uncertainties, and we cannot assure you that the benefits we anticipate will be realized at all or as quickly as we expect. If we don't achieve those benefits, our costs could increase, our expected net income could decrease, and the combined company's future business, financial condition, operating results, and prospects could suffer.***
>
> Our future results will suffer if we do not effectively manage our expanded operations. ***With completion of the Starwood Combination, the size of our business has increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that

we currently anticipate.

309. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

310. The Q3 2016 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Marriott Rewards and The Ritz-Carlton Rewards programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> * * *
>
> ***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements***

***imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms.

* * *

***Any disruption in the functioning of our reservation system, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage a global reservation system that communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

311. These statements and omissions were false and misleading when made because

while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg, and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

312. Attached to the Company's Q3 2016 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

313. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q3 2016 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. In addition, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

**Q. 2016 Form 10-K**

314. On February 21, 2017, the Company filed its Form 10-K for year ending 2016 ("2016 Form 10-K"). The 2016 Form 10-K was signed by Defendants Sorenson, Oberg, Bauduin, the Audit Committee Defendants, and Defendants JW Marriott, Duncan, Harrison, Hippeau, Lee, Reinemund and Schwab and made representations regarding the security of customer data, the Company's operations, the Merger, and other topics.

315. The 2016 Form 10-K repeated the statement from the 2015 Form 10-K that:

> Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***the integrity and protection of customer, employee, and company data is critical to us*** as we use such data for business decisions and to maintain operational efficiency.

316. These statements and omissions concerning the "***integrity and protection***" of data being "***critical***" to the Company were false and misleading when made because at the time Defendants made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants knowingly, or with severe recklessness, failed to share this important information with the market. Further, the legacy Starwood guest reservation database was already compromised by the Data Breach.

317. Further, the statements and omissions: (1) gave the market/investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; (2) gave the market/investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. In addition, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, which now included the fact that the Company's Audit

Department rated the Company as Needs Improvement for cybersecurity and an increase in the volume and severity of cyberattacks in the hospitality industry, however, Defendants ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, which the Director Defendants now knew included the fact that Starwood did not mandate PCI compliance, nor did Starwood use tokenization or point-to-point encryption, and that Starwood's systems posed a higher risk to the Company, as detailed in Section VII.B.(3); (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of GDPR. *See* Section VII.H.(4).

318. The 2016 Form 10-K described **potential** risks the Company **might** face as a result of the Merger:

> We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner, and we cannot assure you that those benefits will be realized at all or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and our future business, financial condition, operating results, and prospects could suffer.
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each company's ongoing businesses, processes, and systems or inconsistencies in standards, controls, procedures, practices, policies, and compensation arrangements could adversely affect the combined company. We may also have difficulty addressing differences in corporate cultures and management philosophies, and in harmonizing our different reservations and other systems and business practices. Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time***

> ***offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.***
>
> *Our future results will suffer if we do not effectively manage our expanded operations.* ***With completion of the Starwood Combination, the size of our business has increased significantly. Our continued success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.

319. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

320. The 2016 Form 10-K described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty Programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***

* * *

***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

* * *

***Any disruption in the functioning of our reservation system, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage a global reservation system that***

***communicates reservations to our branded hotels that individuals make directly with us online, through our mobile app, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation system are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation system. In addition, the risk of disruption in the functioning of our global reservation system could increase in connection with the system integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation system could result in a disruption to our business and the loss of important data.***

321. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

322. Attached to the Company's 2016 Form 10-K were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 268.

323. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the 2016 Form 10-K, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

**R. <u>Conference Call, dated March 21, 2017</u>**

324. On March 21, 2017, the Company held a conference call. During the conference

call, Defendant Linnartz discussed Starwood's IT systems and the "access to the legacy Starwood accounts and customer information globally" and informed the market that they were "still mining the data."

**S. First Quarter 2017 Form 10-Q**

325. On May 9, 2017, the Company filed its first quarter 2017 Form 10-Q ("Q1 2017 Form 10-Q"), which was signed by Defendant Bauduin. The Q1 2017 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner, and we cannot assure you that those benefits will be realized at all or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and our future business, financial condition, operating results, and prospects could suffer.
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each company's ongoing businesses, processes, and systems or inconsistencies in standards, controls, procedures, practices, policies, and compensation arrangements could adversely affect the combined company. We may also have difficulty addressing differences in corporate cultures and management philosophies, and in harmonizing our different reservations and other systems and business practices.*** Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.
>
> *Our future results will suffer if we do not effectively manage our expanded operations.* ***With completion of the Starwood Combination, the size of our business has increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.

326. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee Defendants were specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made because at the time Defendants Bauduin, Oberg and Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants Bauduin, Oberg and Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

327. Further, the statements and omissions: (1) gave investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; (2) gave investors a false impression

that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, which now included the fact that the Company's Audit Department rated the Company as Needs Improvement for cybersecurity and an increase in the volume and severity of cyberattacks in the hospitality industry, however, Defendants ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, which the Director Defendants now knew included the fact that Starwood did not mandate PCI compliance, nor did Starwood use tokenization or point-to-point encryption, and that Starwood's systems posed a higher risk to the Company than Marriott's, and that PwC recommended enhanced network segmentation, two-factor authentication, and vulnerability remediation for Starwood's systems, as detailed in Section VII.B.(3) and (4) and G; (2) significant (and public) intrusions into the systems and databases of Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of GDPR. *See* Section VII.H.(4).

328. The Q1 2017 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer.***

***We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***

* * *

***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access to such systems have increased significantly in recent years. ***A significant theft, loss, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

* * *

> ***Any disruption in the functioning of our reservation systems, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase in connection with the systems integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

329. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

330. Attached to Marriott's Q1 2017 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

331. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q1 2017 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and

omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

**T. Form 8-K, dated August 7, 2017**

332. On August 7, 2017, the Company filed a Form 8-K signed by Defendant Bauduin and attached a press release reporting the Company's operations, the Integration, and other topics. Defendant Sorenson stated: "***Integration of the Starwood transaction is on track.***"

333. This statement and/or omission that the Integration was currently "***on track***" at that point was false and misleading when made for the reasons detailed in ¶¶ 259-260.

**U. Second Quarter 2017 Form 10-Q**

334. On August 8, 2017, the Company filed the Company's second quarter 2017 Form 10-Q ("Q2 2017 Form 10-Q"), which was signed by Defendant Bauduin. The Q2 2017 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> We may not be able to integrate Starwood successfully and many of the anticipated benefits of combining Starwood and Marriott may not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Achieving those anticipated benefits is subject to a number of uncertainties, including whether we can integrate the business of Starwood in an efficient and effective manner, and we cannot assure you that those benefits will be realized as fully or as quickly as we expect.*** If we do not achieve those benefits, our costs could increase, our expected net income could decrease, and our future business, financial condition, operating results, and prospects could suffer.
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each company's ongoing businesses, processes, and systems or inconsistencies in standards, controls, procedures, practices, policies, and compensation arrangements could adversely affect the combined company. We may also have difficulty addressing differences in corporate cultures and management philosophies, and in harmonizing our different reservations and other systems and business practices.*** Although we expect that the elimination of certain duplicative costs, as well as the realization of other efficiencies related to the integration of the two businesses, will over time offset the substantial incremental transaction and merger-related costs and charges we incurred in connection with the Starwood Combination, we may not achieve this net benefit in the near term, or at all.

> *Our future results will suffer if we do not effectively manage our expanded operations.* ***With completion of the Starwood Combination, the size of our business increased significantly. Our future success depends, in part, upon our ability to manage this expanded business, which poses substantial challenges for management, including challenges related to the management and monitoring of new operations and associated increased costs and complexity.*** We cannot assure you that we will be successful or that we will realize the expected operating efficiencies, cost savings, and other benefits from the combination that we currently anticipate.

335. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

336. The Q2 2017 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty Programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> * * *
>
> ***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we***

***maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have increased significantly in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

* * *

***Any disruption in the functioning of our reservation systems, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other***

> ***distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase in connection with the systems integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

337. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

338. Attached to Marriott's Q2 2017 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

339. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q2 2017 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

## V. Marriott's Privacy Statement

340. On September 23, 2016, the Company completed the acquisition of Starwood. On October 5, 2017, the Company updated the Online Privacy Statement. The Company informed the market of its policy for transferring, storing, and securing the customer data the Company

collected through starwoodhotels.com:

> **SAFE HARBOR**
>
> In addition, Starwood is certified under the Safe Harbor privacy framework as set forth by the U.S. Department of Commerce, European Commission and Switzerland regarding the collection, storage, use, transfer and other processing of PII transferred from the European Economic Area or Switzerland to the U.S. Please note that since October 6, 2015, the European Union no longer recognizes Safe Harbor. ***Nonetheless, Starwood upholds to comply with the Safe Harbor Privacy Principles.***
>
> **DELETION AND RETENTION OF YOUR PERSONAL DATA**
>
> ***Your personal data will be kept in a form which enables to identify you for no longer than it is necessary for the purposes for which we collected and use your data.*** Your personal data may be retained in certain files for a period of time as required by applicable law and following Starwood's data retention policies in order to comply with such financial or legal requirements, to properly resolve disputes or to troubleshoot problems. In addition, some types of information may be stored indefinitely due to technical constraints, and will be blocked from further processing for purposes which are not mandatory by law.
>
> * * *
>
> **SECURITY SAFEGUARDS**
>
> ***Starwood recognizes the importance of information security, and is constantly reviewing and enhancing our technical, physical, and logical security rules and procedures. All Starwood owned web sites and servers have security measures in place to help protect your personal data against accidental, loss, misuse, unlawful or unauthorized access, disclosure, or alteration while under our control. Although "guaranteed security" does not exist either on or off the Internet, we safeguard your information using appropriate administrative, procedural and technical safeguards, including password controls, "firewalls" and the use of up to 256-bit encryption based on a Class 3 Digital Certificate issued by VeriSign, Inc. This allows for the use of Secure Sockets Layer (SSL), an encryption method used to help protect your data from interception and hacking while in transit.***

341. These statements and omissions concerning Starwood's, and thus the Company's, information and data security were false and misleading when made because at this time, the Company was in violation of the Safe Harbor Principles that Defendants stated the Company adhered to. These statements and omissions were also false and misleading when made for the

reasons detailed in ¶¶ 259-260.

**W. Third Quarter 2017 Form 10-Q**

342. On November 8, 2017, the Company filed the Company's third quarter 2017 Form 10-Q ("Q3 2017 Form 10-Q"), which was signed by Defendant Bauduin. At the time of the filing of the Q3 2017 Form 10-Q, the Merger had already closed and the Company owned the legacy Starwood guest reservation database.

343. The Q3 2017 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> Some of the anticipated benefits of combining Starwood and Marriott may still not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to a number of uncertainties, including whether we can continue to integrate the business of Starwood in an efficient and effective manner and whether, and on what terms, we can reach agreement with the companies that issue our branded credit cards and the timeshare companies with whom we do business to allow us to move to a single unified reservation system and loyalty platform.***
>
> ***The integration process could take longer than we anticipate and involve unanticipated costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems and business practices as the integration process continues.*** As a result of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits.

344. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk

disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

345. The Q3 2017 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, and property management systems, our Loyalty Programs, and technologies we make available to our guests. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and if we cannot do so as quickly as our competitors or within budgeted costs and time frames, our business could suffer. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> * * *
>
> ***We are exposed to risks and costs associated with protecting the integrity and security of internal and customer data. Our businesses process, use, and transmit large volumes of internal employee and customer data, including credit card numbers and other personal information in various information systems that we maintain*** and in those maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that customer, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our customers and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by governmental regulation and the requirements of the payment card industry are also increasingly demanding, in both the United States and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing requirements and employee and customer expectations, or may require significant additional investments or time in order to do so.***
>
> ***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or***

> ***inadvertent releases of data may materially impact our, including our owners', franchisees', licensees', or service providers', information systems and records.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have increased significantly in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.
>
> * * *
>
> ***Any disruption in the functioning of our reservation systems, such as in connection with our integration of Starwood, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, or through our telephone call centers, or through intermediaries like travel agents, Internet travel websites and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase in connection with the systems integration that we anticipate undertaking as part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

346. These statements were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure

requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

347. Attached to Marriott's Q3 2017 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

348. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q3 2017 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

## X. Third Quarter 2017 Earnings Call

349. On November 8, 2017, the Company held a conference call to discuss the Company's operations, the Integration, and other topics. Defendant Sorenson stated:

> We've never been more optimistic about our business, our underlying competitive strengths and our long-term growth potential. ***The Starwood integration is on track.*** We have identified more synergies and more business opportunities than we anticipated. We continue to believe we will achieve $250 million of G&A savings and expect to do that in 2018. And we continue to improve our products, services and systems to enhance the value of every room night.

350. These statements and omissions that the Integration was currently "***on track***" at that point were false and misleading when made for the reasons detailed in ¶¶ 259-260.

## Y. Defendant Hoffmeister Interview

351. On January 12, 2018, Defendant Hoffmeister conducted an interview with Rich Siegel to discuss the Merger, and other topics. Defendant Hoffmeister was asked about the Integration process, and in response misleadingly stated that the Company was utilizing the "***best***" of Starwood's systems and that Marriott had conducted a "thorough analysis" of Starwood's

systems:

> Siegel
>
> It's been more than a year since Marriott International merged with Starwood. From your perspective, how's the integration process going?
>
> Defendant Hoffmeister
>
> Whenever two large companies come together, you have to determine what processes, systems and tools to use. ***We're going through the process of bringing our systems together to get the best of both worlds wherever possible.*** It's very exciting. We have a lot going on, and a lot of work ahead still, but it's a very exciting time.
>
> * * *
>
> Siegel
>
> At the Download conference, you mentioned that when you learned of the Starwood merger, as CIO you looked for advice from other CIOs. Can you elaborate on that?
>
> Defendant Hoffmeister
>
> * * *
>
> Two themes emerged. The first was quite simply to "just adopt and go." Choose your systems and just go with them; you're not going to please everyone. ***We did a thorough analysis of the systems before we made our decision***, but we didn't dwell on it, we just made a decision.

352. These statements and omissions concerning the Company getting "***the best of both worlds***" through the Merger, and the Company's purported "***thorough analysis***" of Starwood's systems were false and misleading when made because at the time Defendant Hoffmeister made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no

record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendant Hoffmeister knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

353. Further, the statements and omissions: (1) gave investors a false impression that the Company had undertaken sufficient due diligence, and was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; (2) gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, which now included the fact that the Company's Audit Department rated the Company as Needs Improvement for cybersecurity and an increase in the volume and severity of cyberattacks in the hospitality industry, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the

passage and imminent enforcement of GDPR. *See* Section VII.H.(4).

**Z. 2017 Form 10-K**

354. On February 15, 2018, the Company filed its 2017 Form 10-K. The 2017 Form 10-K was signed by Defendants Sorenson, Oberg, and Bauduin, the Audit Committee Defendants, and Defendants JW Marriott, Duncan, Harrison, Hippeau, Lee, Reinemund, and Schwab and made representations regarding the security of customer data, the Company's operations, the Integration, and other topics.

355. In the 2017 Form 10-K, the Company stated:

> Keeping pace with developments in technology is important for our operations and our competitive position. Furthermore, ***the integrity and protection of customer, employee, and company data is critical to us*** as we use such data for business decisions and to maintain operational efficiency.

356. These statements and omissions concerning the "***integrity***" and "***protection***" of data being "***critical***" to Marriott were false and misleading when made for the reasons stated in ¶¶ 259-260.

357. The 2017 Form 10-K described **potential** risks the Company **might** face as a result of the Merger:

> Some of the anticipated benefits of combining Starwood and Marriott may still not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business and whether, and on what terms, we can reach agreement with the timeshare companies with whom we do business to allow us to move to a single unified reservation system and loyalty platform.***
>
> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems and business practices as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize

> additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits.

358. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Sorenson, Oberg, and Bauduin, the Audit Committee Defendants, and Defendants JW Marriott, Duncan, Harrison, Hippeau, Lee, Reinemund, and Schwab failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

359. The 2017 Form 10-K described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> * * *
>
> ***We are exposed to risks and costs associated with protecting the integrity and security of company associate and guest data. Our businesses process, use, and transmit large volumes of associate and guest data, including credit card numbers and other personal information in various information systems that we maintain*** and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic

communications. ***The integrity and protection of that guest, associate, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our guests and associates also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and employee and guest expectations, or may require significant additional investments or time to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

* * *

***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing***

> ***our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the anticipated systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

360. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Sorenson, Oberg, and Bauduin, the Audit Committee Defendants, and Defendants JW Marriott, Duncan, Harrison, Hippeau, Lee, Reinemund, and Schwab failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

361. Attached to Marriott's 2017 Form 10-K were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 268.

362. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the 2017 Form 10-K, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

### AA. First Quarter 2018 Form 10-Q

363. On May 10, 2018, the Company filed the Company's first quarter 2018 Form 10-Q ("Q1 2018 Form 10-Q"), which was signed by Defendant Bauduin. The Q1 2018 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> Some of the anticipated benefits of combining Starwood and Marriott may still not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination will result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business.***
>
> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems, Loyalty Programs and other business practices as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits, or that difficulties encountered with our harmonization efforts will not have adverse effects on our business or reputation.

364. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. Additionally, these statements were false and misleading when made because at the time Defendants made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored

without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants Bauduin, Oberg and Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. Further, the legacy Starwood guest reservation database was already compromised by the Data Breach.

365. Further, the statements and omissions: (1) gave investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; and (2) gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E.; and (4) the passage and imminent enforcement of GDPR. *See* Section VII.H.(4). Additionally, on February 21, 2018, the SEC released guidance for companies specifically on disclosing cybersecurity risk.

366. The Q1 2018 Form 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***

* * *

***We are exposed to risks and costs associated with protecting the integrity and security of company, employee, and guest data. Our businesses process, use, and transmit large volumes of employee and guest data, including credit card numbers and other personal information in various information systems that we maintain*** and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that guest, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***

***Our guests and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and employee and guest expectations, or may require significant additional investments or time to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, employee,***

***or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits, and negative publicity, resulting in tangible adverse effects on our business, including consumer boycotts, lost sales, litigation, loss of development opportunities, or associate retention and recruiting difficulties, all of which could affect our market share, reputation, business, financial condition, or results of operations. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage information systems change frequently, can be difficult to detect for long periods of time, and can be difficult to assess ore remediate even once detected, which could magnify the severity of these adverse effects.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

* * *

***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the anticipated systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

367. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk

disclosure requirements. These statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-260.

368. Attached to Marriott's Q1 2018 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

369. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q1 2018 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

**BB. Global Privacy Statement, dated May 18, 2018**

370. As of May 18, 2018, the Company provided the public with a Global Privacy Statement. In the Global Privacy Statement, the Company stressed its policies and procedures for using, collecting, and storing the data the Company collects from its customers. The Global Privacy Statement stated:

> Security
>
> ***We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the "Contacting Us" section, below.
>
> Privacy Shield Certified
>
> ***Marriott International, Inc. and certain of its U.S. affiliates have certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks***. Our certifications can be found at: www.privacyshield.gov/list. For more information about the Privacy Shield principles, please visit: www.privacyshield.gov. Our Privacy Shield Guest Privacy Policy can be found here.

### CC. Second Quarter 2018 Form 10-Q

371. On August 7, 2018, the Company filed the Company's second quarter 2018 Form 10-Q ("Q2 2018 Form 10-Q"), which was signed by Defendant Bauduin. The Q2 2018 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> Some of the anticipated benefits of combining Starwood and Marriott may still not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination would result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business.***
>
> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We also may still encounter difficulties harmonizing our different reservations and other systems, Loyalty Programs and other business practices as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits, or that difficulties encountered with our harmonization efforts will not have adverse effects on our business or reputation.

372. These statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. Additionally, these statements and omissions were false and misleading when made because while warning of potential risks related to integrating the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. These statements were false and misleading when made because at the time Defendants Bauduin, Oberg

and Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants Bauduin, Oberg and Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

373. Further, the statements and omissions: (1) gave investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above, which now included the enforcement of GDPR; and (2) gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client

data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; and (3) other significant data breaches in other industries, as detailed in Section VII.E.. Additionally, on February 21, 2018, the SEC released guidance for companies specifically on disclosing cybersecurity risk.

374. The Q2 2018 10-Q described **potential** risks the Company **might** face as a result of its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Programs, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***
>
> * * *
>
> ***We are exposed to risks and costs associated with protecting the integrity and security of company, employee, and guest data. Our businesses process, use, and transmit large volumes of employee and guest data, including credit card numbers and other personal information in various information systems that we maintain*** and in systems maintained by third parties, including our owners, franchisees and licensees, as well as our service providers, in areas such as human resources outsourcing, website hosting, and various forms of electronic communications. ***The integrity and protection of that guest, employee, and company data is critical to our business. If that data is inaccurate or incomplete, we could make faulty decisions.***
>
> ***Our guests and employees also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation and the requirements of the***

***payment card industry are also increasingly demanding, in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and associate and guest expectations, or may require significant additional investments or time to do so.***

***Cyber-attacks could have a disruptive effect on our business. Efforts to hack or breach security measures, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers.*** Our reliance on computer, Internet-based and mobile systems and communications and the frequency and sophistication of efforts by hackers to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. ***A significant theft, loss, loss of access to, or fraudulent use of guest, associate, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Breaches in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits, and negative publicity, resulting in tangible adverse effects on our business, including consumer boycotts, lost sales, litigation, loss of development opportunities, or associate retention and recruiting difficulties, all of which could affect our market share, reputation, business, financial condition, or results of operations. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage information systems change frequently, can be difficult to detect for long periods of time, and can be difficult to assess ore remediate even once detected, which could magnify the severity of these adverse effects.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security breaches, and other related breaches. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

* * *

***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing***

> ***our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the anticipated systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

375. These statements and omissions were false and misleading when made because while warning of potential cybersecurity-related risks to the business, Defendants Bauduin, Oberg and Sorenson failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

376. Attached to Marriott's Q2 2018 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶ 292.

377. These statements and omissions were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q1 2018 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

**DD. Marriott's Global Privacy Statement, dated September 19, 2018**

378. On September 19, 2018, the Company continued to provide the public with a Global Privacy Statement on Marriott's website, www.marriott.com. Despite Defendants having actual knowledge of the Data Breach on September 18, 2018, Defendants continued to provide a version of the Global Privacy Statement. In the Global Privacy Statement, the Company provided the

public with its policies and procedures for using, collecting, and storing the data the Company collects from its customers.

> Security
>
> ***We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.*** Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of your account has been compromised), please immediately notify us in accordance with the *"Contacting Us"* section, below.
>
> Privacy Shield Certified
>
> ***Marriott International, Inc. and certain of its U.S. affiliates have certified to the EU-U.S. and Swiss-U.S. Privacy Shield frameworks.*** Our certifications can be found at: www.privacyshield.gov/list. For more information about the Privacy Shield principles, please visit: www.privacyshield.gov. Our Privacy Shield Guest Privacy Policy can be found here.

379. These statements and omissions were false and misleading when made because the Company was in violation of the Privacy Shield Frameworks, which the Company stated it complied with, and despite Defendants having **actual knowledge of the Data Breach**,. Defendants failed to make any change to the Global Privacy Statement as a result. Additionally, these statements and omissions were false and misleading when because while warning of potential risks related to integrating the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing. Additionally, these statements were false and misleading when made because at the time Defendants made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of

remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach.

380. Further, the statements and omissions: (1) gave investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; and (2) gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; and (3) other significant data breaches in other industries, as detailed in Section VII.E.. Additionally, on February 21, 2016, the SEC released guidance for companies specifically on disclosing cybersecurity risk.

**EE. Salesforce's The Future of Travel & Hospitality**

381. On September 25, 2018, Salesforce hosted an event entitled *The Future of Travel & Hospitality*, during which Defendant Sorenson stated:

> [Interviewer]: So what would you say has been your biggest bet when it comes to technology?
>
> Defendant Sorenson: Well, um, that's a good question. I think the, uh, we spend a lot of money on technology. We're spending hundreds of millions of dollars a year. ***Uh, it is mostly about investing in the loyalty and reservations platform. Uh, they're big bets but they are not risky bets . . . .***
>
> ***I think the, uh, biggest bet that sort of has some risk in it . . . was our acquisition of Starwood a couple of years ago. . . $13 billion dollars, biggest deal by a lot that Marriott has ever done. We were a $20 billion company when we bought them so, you know, it's risking a fair amount of the Company***. And while it isn't at its core maybe a technology bet, it was a bet on the loyalty program. We said if we can bring these two companies together and have a bigger ecosystem for our customers, and they are really our customers, then we can say to them, "why would you stay anywhere else?" that would be a good thing.
>
> [Interviewer]: You mentioned risk, what would be some of the riskier elements of technology? . . . .
>
> Defendant Sorenson: . . . . You've got two examples that I'd use today. ***One is the regulatory one. So we are increasingly living in a world in which data will be required to be maintained in the country of residence of your customer. GDPR in Europe is probably the most profound, China heading the same way, California of course passed a law last year. All of this is going to have some impact on where we can keep the information we have about you.*** And to some extent how we mine it. Can we mine it through pure anonymous tools . . . ***so that's an area of risks***.

382. These statements and omissions concerning the Merger, legacy Starwood guest reservation database, and regulatory compliance, made **after** Defendant Sorenson and the Audit Committee Defendants admittedly had **actual knowledge of the Data Breach**, were false and misleading when made because at the time Defendant Sorenson made these statements, Starwood's IT systems were severely vulnerable. Specifically: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed

for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers; and (7) that Starwood did not mandate PCI compliance, tokenization, or point-to-point encryption. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendant Sorenson knowingly, or with severe recklessness, failed to share this important information with the market. In addition, the legacy Starwood guest reservation database was already compromised by the Data Breach, a fact which Defendant Sorenson now had actual knowledge of.

383. Further, the statements and omissions: (1) gave investors a false impression that the Company was operating the newly-acquired Starwood systems in accordance with relevant requirements, standards, and best practices detailed above; and (2) gave investors a false impression that the Company had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, Defendants failed to secure Starwood's systems, despite knowledge of cybersecurity risks. Additionally, as detailed in the Board minutes pleaded in Section VII.G., the Director Defendants were well aware of the risk that cybersecurity posed to the Company, however, they ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the

hospitality industry, as detailed in Section VII.E.; and (3) other significant data breaches in other industries, as detailed in Section VII.E.. Additionally, on February 21, 2016, the SEC released guidance for companies specifically on disclosing cybersecurity risk.

**FF. Skift Global Forum 2018**

384. On October 10, 2018, Defendant Sorenson was interviewed at the Skift Global Forum 2018 by Skift's Senior Hospitality Editor, Deanna Ting. Ms. Ting asked Defendant Sorenson whether there have been "any disappointments along the way" in connection with the Merger. Defendant Sorenson stated:

> ***There has never been a moment of regret. . . . Have there been disappointments? Of course, but there have also been positive surprises. And I think on balance there have been more positive surprises than negative ones.***

385. Defendant Sorenson was also asked about the Company's reservation system:

> Ms. Ting: Speaking of software, reservations systems, I sort of feel like your reservations platform, is overdue for an overhaul. How are you planning to update it or have you already updated it?
>
> Defendant Sorenson: ***Well we are, uh, again, this is a little bit in the context of the merger of Starwood and Marriott, uh right now in waves, we are putting all of the Starwood hotels on the Marriott system. Uh, that will be done at the end of the year, uh then stabilized. We do have a new res platform that's rolling out this year . . . .***

386. These statements and omissions concerning the Merger and the legacy Starwood guest reservation database, made **after** Defendant Sorenson and the Audit Committee Defendants admittedly had **actual knowledge of the Data Breach**, were false and misleading when made for the reasons detailed in ¶¶ 259-60

**GG. Interview with Richmond Times Dispatch**

387. In an article in The New York Times titled *Marriott's Merger of Hotel Rewards Programs Tests Members' Loyalty*, Marriott's Senior VP of Global Loyalty David Flueck gave an interview to the *Richmond Times Dispatch*. In that article, Mr. Flueck "***described the merger as***

***99.9 percent successful***, though he acknowledged that it still left millions of customer records in limbo, some for weeks before they were resolved."

388. This statement and/or omission concerning the success of the Merger, made **after** Defendant Sorenson and the Audit Committee Defendants admittedly had **actual knowledge of the Data Breach**, was false and misleading for the reasons detailed in ¶¶ 259-60

**HH. Form 8-K, dated November 5, 2018**

389. On November 5, 2018, the Company filed a Form 8-K signed by Defendant Bauduin. In regard to the Integration, Defendant Sorenson stated:

> It's been just over two years since the completion of the Starwood acquisition. ***We are in the home stretch on integrating the companies and are pleased with the results.***

390. These statements and omissions concerning the progress and success of the Integration up to that point, made **after** Defendant Sorenson and the Audit Committee Defendants admittedly had **actual knowledge of the Data Breach**, were false and misleading when made for the reasons detailed in ¶¶ 259-60.

**II. Third Quarter 2018 Form 10-Q**

391. On November 6, 2018, the Company filed the Company's third quarter 2018 Form 10-Q ("Q3 2018 Form 10-Q"), which was signed by Defendant Bauduin.

392. The Q3 2018 Form 10-Q described **potential** risks the Company **might** face as a result of the Merger:

> Some of the anticipated benefits of combining Starwood and Marriott may still not be realized. ***We decided to acquire Starwood with the expectation that the Starwood Combination would result in various benefits, including, among other things, operating efficiencies. Although we have already achieved some of those anticipated benefits, others remain subject to several uncertainties, including whether we can continue to effectively and efficiently integrate the Starwood business.***

> ***Integration could also take longer than we anticipate and involve unexpected costs. Disruptions of each legacy company's ongoing businesses, processes, and systems could adversely affect the combined company. We have encountered challenges in harmonizing our different reservations and other systems, Loyalty Program, and other business practices, and may encounter additional or increased challenges as the integration process continues.*** Because of these or other factors, we cannot assure you when or that we will be able to fully realize additional benefits from the Starwood Combination in the form of eliminating duplicative costs, or achieving other operating efficiencies, cost savings, or benefits, or that challenges encountered with our harmonization efforts will not have adverse effects on our business or reputation.

393. These statements and omissions, made **after** Defendant Sorenson and the Audit Committee Defendants admittedly had **actual knowledge of the Data Breach**, were false and misleading when made because while warning of potential risks related to integrating the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-60

394. The Q3 2018 Form 10-Q described **potential** risks the Company **might** face in its technology and information protection operations:

> ***A failure to keep pace with developments in technology could impair our operations or competitive position. The lodging industry continues to demand the use of sophisticated technology and systems, including those used for our reservation, revenue management, property management, human resources and payroll systems, our Loyalty Program, and technologies we make available to our guests and for our associates. These technologies and systems must be refined, updated, and/or replaced with more advanced systems on a regular basis, and our business could suffer if we cannot do that as quickly or effectively as our competitors or within budgeted costs and time frames. We also may not achieve the benefits that we anticipate from any new technology or system, and a failure to do so could result in higher than anticipated costs or could impair our operating results.***

* * *

***We are exposed to risks and costs associated with protecting the integrity and security of company, associate, and guest data. In the operation of our business, we collect, store, use, and transmit large volumes of data regarding associates, guests, customers, owners, licensees, franchisees, and our own business operations, including credit card numbers, reservation and loyalty data, and other personal information, in various information systems that we maintain*** and in systems maintained by third parties, including our owners, franchisees, licensees, and service providers. ***The integrity and protection of this data is critical to our business. If this data is inaccurate or incomplete, we could make faulty decisions.***

***Our guests and associates also have a high expectation that we, as well as our owners, franchisees, licensees, and service providers, will adequately protect and appropriately use their personal information. The information, security, and privacy requirements imposed by laws and governmental regulation, our contractual obligations, and the requirements of the payment card industry are also increasingly demanding in the U.S., the European Union, Asia, and other jurisdictions where we operate. Our systems and the systems maintained or used by our owners, franchisees, licensees, and service providers may not be able to satisfy these changing legal and regulatory requirements and associate and guest expectations, or may require significant additional investments or time to do so. We may incur significant additional costs to meet these requirements, obligations, and expectations, and in the event of alleged or actual noncompliance we may experience increased operating costs, increased exposure to fines and litigation, and increased risk of damage to our reputation and brand.***

* * *

***Cyber security incidents could have a disruptive effect on our business. We have implemented security measures to safeguard our systems and data, and we may implement additional measures in the future, but our measures or the measures of our service providers or our owners, franchisees, licensees, and their service providers may not be sufficient to maintain the confidentiality, security, or availability of the data we collect, store, and use to operate our business. Efforts to hack or circumvent security measures, efforts to gain unauthorized access to data, failures of systems or software to operate as designed or intended, viruses, "ransomware" or other malware, "phishing" or other types of business email compromises, operator error, or inadvertent releases of data may materially impact our information systems and records and those of our owners, franchisees, licensees, or service providers. Our reliance on computer, Internet-based, and mobile systems and communications and the frequency and sophistication of efforts by third parties to gain unauthorized access or prevent authorized access to such systems have greatly increased in recent years. Like most large multinational corporations, we have experienced cyber-attacks, attempts to disrupt access to our systems and data, and attempts to affect the integrity of our data, and the frequency and sophistication of such efforts could***

***continue to increase. Although some of these efforts may not be successful or impactful, a significant theft, loss, loss of access to, or fraudulent use of guest, associate, owner, franchisee, licensee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation. Depending on the nature and scope of the event, compromises in the security of our information systems or those of our owners, franchisees, licensees, or service providers or other disruptions in data services could lead to an interruption in the operation of our systems, resulting in operational inefficiencies and a loss of profits, and negative publicity, resulting in tangible adverse effects on our business, including consumer boycotts, lost sales, litigation, loss of development opportunities, or associate retention and recruiting difficulties, all of which could affect our market share, reputation, business, financial condition, or results of operations. The techniques used to obtain unauthorized access, disable or degrade service, or sabotage information systems change frequently, can be difficult to detect for long periods of time, and can involve difficult or prolonged assessment or remediation periods even once detected, which could magnify the severity of these adverse effects.*** In addition, although we carry cyber/privacy liability insurance that is designed to protect us against certain losses related to cyber risks, that insurance coverage may not be sufficient to cover all losses or all types of claims that may arise in connection with cyber-attacks, security compromises, and other related incidents. Furthermore, in the future such insurance may not be available to us on commercially reasonable terms, or at all.

***Any disruption in the functioning of our reservation systems, as part of our integration of Starwood or otherwise, could adversely affect our performance and results. We manage global reservation systems that communicate reservations to our branded hotels that individuals make directly with us online, through our mobile apps, through our telephone call centers, or through intermediaries like travel agents, Internet travel websites, and other distribution channels. The cost, speed, accuracy and efficiency of our reservation systems are critical aspects of our business and are important considerations for hotel owners when choosing our brands. Our business may suffer if we fail to maintain, upgrade, or prevent disruption to our reservation systems. In addition, the risk of disruption in the functioning of our global reservation systems could increase with the ongoing systems integration that is part of our integration of Starwood. Disruptions in or changes to our reservation systems could result in a disruption to our business and the loss of important data.***

395. These statements and omissions, made **after** Defendant Sorenson and the Audit Committee Defendants had **actual knowledge of the Data Breach**, were false and misleading when made because while warning of potential risks related to integrating the business, Defendants failed to disclose critical facts relevant to these risks that existed at the time, including the

vulnerability of the customer data and that the Data Breach was currently ongoing, despite the fact that the Audit Committee was specifically advised regarding the SEC's risk disclosure requirements. Additionally, these statements and omissions were false and misleading when made for the reasons detailed in ¶¶ 259-60

396. Attached to Marriott's Q3 2018 Form 10-Q were SOX Certifications signed by Defendants Sorenson and Oberg with statements identical to those detailed in ¶¶ 292.

397. These statements and omissions, made **after** Defendant Sorenson and the Audit Committee Defendants had **actual knowledge of the Data Breach**, were false and misleading when made because either Defendants Sorenson and Oberg reviewed the Q3 2018 Form 10-Q, and knew they could not reasonably certify that the risk language was not false and misleading, or they were at least severely reckless in certifying that it was not false and misleading given the information available to them at the time concerning the risks that existed to the customer data. These statements and omissions were also false and misleading when made for the reasons detailed in ¶¶ 259-260.

## X. MATERIALLY FALSE AND MISLEADING PROXY STATEMENTS

### A. 2017 Proxy Statement

398. On April 5, 2017, the Company filed a Schedule 14A filed with the SEC (the "2017 Proxy Statement"). Defendants Sorenson, J.W. Marriott, Duncan, Harrison, Henderson, Hippeau, Kellner, Lee, Lewis, Muñoz, Reinemund, and Schwab solicited the 2017 Proxy Statement filed pursuant to Section 14(a) of the Exchange Act, which contained material misstatements and omissions.[18]

[18] Plaintiffs' allegations with respect to the misleading statements in the 2017 Proxy Statement are based solely on negligence; they are not based on any allegation of reckless or knowing conduct by or on behalf of Defendants, and they do not allege, and do not sound in, fraud. Plaintiffs specifically disclaim any allegations of, reliance upon any allegation of, or reference to any allegation of fraud, scienter, or

399. Regarding the Company's Code of Ethics, the 2017 Proxy Statement noted that:

> The Company has long maintained and enforced a Code of Ethics that applies to all Marriott associates, including our Chairman of the Board, Chief Executive Officer, Chief Financial Officer and Principal Accounting Officer and to each member of the Board. The Code of Ethics is encompassed in our Business Conduct Guide, which is available in the Investor Relations section of our website (www.marriott.com/investor) by clicking on "Corporate Governance" and then "Documents & Charters." We will post on that website any future changes or amendments to our Code of Ethics, and any waiver of our Code of Ethics that applies to our Chairman of the Board, any of our executive officers, or a member of our Board within four business days following the date of the amendment or waiver.

400. The 2017 Proxy Statement was false and misleading because, despite assertions to the contrary, its Code of Ethics was not followed, as Defendants conducted little, if any, oversight of the Company's engagement in Defendants' scheme to issue materially false and misleading statements to the public and to facilitate and disguise Defendants' violations of law, failed to maintain the accuracy of Company records and reports, comply with laws and regulations, protect customer information and the Company's reputation, or conduct business in an honest and ethical manner. Further, multiple Defendants violated the code by selling shares of Company stock while in possession of material, non-public information about the Company.

401. Defendants also caused the 2017 Proxy Statement to be false and misleading with regard to executive compensation in that they purported to employ "pay-for-performance" elements, including stock awards based on earnings per share, while failing to disclose that such measures were being artificially inflated by Defendants' false and misleading statements and repurchases of Company stock, and therefore any compensation based on the Company's financial performance was artificially inflated.

402. The 2017 Proxy Statement also failed to disclose that: (1) the Company did not

---

recklessness with regard to these allegations and related claims.

maintain customer's personal data on a secure system; (2) unknown actors had gained unauthorized access to Starwood's network since 2014; (3) Marriott's due diligence in the Merger failed to discover the Data Breach; (4) the Data Breach caused personal information of up to 500 million guests to be exposed; (5) the Company failed to maintain internal controls; and (6) as a result of the foregoing the Company's public statements were materially false and misleading at all relevant times.

**B. 2018 Proxy Statement**

403. On April 5, 2018, the Company filed a Schedule 14A filed with the SEC (the "2018 Proxy Statement"). Defendants Sorenson, J.W. Marriott, Duncan, Harrison, Henderson, Hippeau, Kellner, Lee, Lewis, Muñoz, Reinemund, and Schwab solicited the 2018 Proxy Statement filed pursuant to Section 14(a) of the Exchange Act, which contained material misstatements and omissions.[19]

404. Regarding the Company's Code of Ethics, the 2018 Proxy Statement noted that:

> The Company has long maintained and enforced a Code of Ethics that applies to all Marriott associates, including our Chairman of the Board, Chief Executive Officer, Chief Financial Officer and Principal Accounting Officer and to each member of the Board. The Code of Ethics is encompassed in our Business Conduct Guide, which is available in the Investor Relations section of our website (www.marriott.com/investor) by clicking on "Corporate Governance" and then "Documents & Charters." We will post on that website any future changes or amendments to our Code of Ethics, and any waiver of our Code of Ethics that applies to our Chairman of the Board, any of our executive officers, or a member of our Board within four business days following the date of the amendment or waiver.

405. The 2018 Proxy Statement was false and misleading because, despite assertions to

[19] Plaintiffs' allegations with respect to the misleading statements in the 2018 Proxy Statement are based solely on negligence; they are not based on any allegation of reckless or knowing conduct by or on behalf of Defendants, and they do not allege, and do not sound in, fraud. Plaintiffs specifically disclaim any allegations of, reliance upon any allegation of, or reference to any allegation of fraud, scienter, or recklessness with regard to these allegations and related claims.

the contrary, its Code of Ethics was not followed, as Defendants conducted little, if any, oversight of the Company's engagement in Defendants' scheme to issue materially false and misleading statements to the public and to facilitate and disguise Defendants' violations of law, failed to maintain the accuracy of Company records and reports, comply with laws and regulations, protect customer information and the Company's reputation, or conduct business in an honest and ethical manner. Further, multiple Defendants violated the code by selling shares of Company stock while in possession of material, non-public information about the Company.

406. Defendants also caused the 2018 Proxy Statement to be false and misleading with regard to executive compensation in that they purported to employ "pay-for-performance" elements, including stock awards based on earnings per share, while failing to disclose that such measures were being artificially inflated by Defendants' false and misleading statements and repurchases of Company stock, and therefore any compensation based on the Company's financial performance was artificially inflated.

407. Further, the 2018 Proxy Statement revealed that the Company approved bonuses for certain named executive officers, including $1 million for Defendant Sorensen, "to reward senior management for its outstanding performance in 2017 regarding the ongoing seamless integration of Starwood." Such bonuses were unwarranted and unjustified as a result of the breaches of fiduciary duty in evaluating and approving the Merger, which led the Company to fail to uncover a data breach that had been ongoing for over a year and would subject the Company to significant expenses and liabilities. Regarding these bonuses, the 2018 Proxy Statement stated, in relevant part:

> ***Taking into consideration*** the unique nature of the Starwood combination and ***the Company's success in maintaining strong quality and brand control over our legacy Marriott operations while maintaining the brand reputation and managing the successful integration of the Starwood operations, and the***

> ***management team's success in building stockholder value through this transformative merger, the [Compensation and Policy] Committee approved a one-time supplemental cash bonus for 2017 in the amount of $500,000 to each of the NEOs and the Board approved a one-time supplemental cash bonus for 2017 in the amount of $1,000,000 for Mr. Sorenson.*** The purpose of the bonus is ***to reward senior management for its outstanding performance in 2017 regarding the ongoing seamless integration of Starwood*** while promoting strong performance in the Company's legacy operations. In particular, the Board cited strong performance across a broad array of criteria, including high levels of associate engagement, human capital development, completion of co-branded credit card deals, successful asset sales, work toward linking and combining loyalty programs, and progress toward improved leverage in the competitive marketplace. . . . The supplemental cash bonus amounts were determined by the Committee with the objective that the award would result in compensation for each of the NEOs that is well-aligned with the Company's pay-for-performance philosophy and exceptionally strong 2017 performance.
> [Emphasis added]

408. The 2018 Proxy Statement also failed to disclose that: (1) the Company did not maintain customer's personal data on a secure system; (2) unknown actors had gained unauthorized access to Starwood's network since 2014; (3) Marriott's due diligence in the Merger failed to discover the Data Breach; (4) the Data Breach caused personal information of up to 500 million guests to be exposed; (5) the Company failed to maintain internal controls; and (6) as a result of the foregoing the Company's public statements were materially false and misleading at all relevant times.

## XI. THE TRUTH EMERGES

409. On November 30, 2018, Marriott published a press release titled "Marriott Announces Starwood Guest Reservation Database Security Incident" which disclosed that it suffered a data breach which exposed the personal information of up to 500 million of its guests and which has been ongoing since 2014. This press release states:

> Marriott has taken measures to investigate and address a data security incident involving the Starwood guest reservation database. On November 19, 2018, the investigation determined that there was unauthorized access to the database, which contained guest information relating to reservations at Starwood properties on or

before September 10, 2018.

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States. Marriott quickly engaged leading security experts to help determine what occurred. ***Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014***. The company recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

***The company has not finished identifying duplicate information in the database, but believes it contains information on up to approximately 500 million guests who made a reservation at a Starwood property***. For approximately 327 million of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information.

Marriott reported this incident to law enforcement and continues to support their investigation. The company has already begun notifying regulatory authorities.

***"We deeply regret this incident happened," said Arne Sorenson, Marriott's President and Chief Executive Officer. "We fell short of what our guests deserve and what we expect of ourselves***. We are doing everything we can to support our guests, and using lessons learned to be better moving forward."

"Today, Marriott is reaffirming our commitment to our guests around the world. We are working hard to ensure our guests have answers to questions about their personal information, with a dedicated website and call center. We will also continue to support the efforts of law enforcement and to work with leading security experts to improve. Finally, we are devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network," Mr. Sorenson continued. [Emphasis added]

410. The press release also revealed that the Company would take the following steps in response to the data breach (the "Response Measures"):

**Dedicated Website and Call Center**

We have established a dedicated website (info.starwoodhotels.com) and call center to answer questions you may have about this incident. The frequently-asked questions on info.starwoodhotels.com may be supplemented from time to time. The call center is open seven days a week and is available in multiple languages. Call volume may be high, and we appreciate your patience.

**Email Notification**

Marriott will begin sending emails on a rolling basis starting today, November 30, 2018, to affected guests whose email addresses are in the Starwood guest reservation database.

**Free WebWatcher Enrollment**

Marriott is providing guests the opportunity to enroll in WebWatcher free of charge for one year. WebWatcher monitors internet sites where personal information is shared and generates an alert to the consumer if evidence of the consumer's personal information is found. Due to regulatory and other reasons, WebWatcher or similar products are not available in all countries. Guests from the United States who activate WebWatcher will also be provided fraud consultation services and reimbursement coverage for free. To activate WebWatcher, go to info.starwoodhotels.com and click on your country, if listed, for enrollment.

411. On information and belief, Plaintiffs allege that Defendants were informed of and approved the announced Dedicated Website and Call Center, Email Notification, and Free WebWatcher Enrollment.

412. Defendants knew or recklessly disregarded the weaknesses of its implemented email notification procedure. As discussed in a December 3, 2018 Techcrunch.com article titled "Marriott's breach response is so bad, security experts are filling in the gaps-at their own expense", these weaknesses include that the email's sender domain does not look like a legitimate domain because the domain does not load to a website or have an identifying HTTPS certificate and that the email is easily spoofable (*i.e.*, easy for cyber squatters to register similar-looking domain names).

413. Defendants knew or recklessly disregarded the weaknesses of its implemented

dedicated website and call center. By way of example, in Marriott's November 30, 2018 press release it stated "[t]o WebWatcher, go to info.starwoodhotels.com and click on your country, if listed, for enrollment. However, if one attempts to "click" on USA to enroll in WebWatcher, he/or she will discover there is no accessible link. And WebWatcher is not readily identifiable on this webpage.

414. On November 30, 2018, Marriott filed a Form 8-K with the SEC relating to the Data Breach. In addition to attaching the press release discussed above (*see* ¶ 409, Marriott included answers to what it represented were "…certain frequently asked questions related to the cybersecurity incident…", stating:

> What will be the financial impact to the Company from this cybersecurity incident?
>
> It is premature to estimate the financial impact to the Company. The Company carries insurance, including cyber insurance, commensurate with its size and the nature of its operations. The Company is working with its insurance carriers to assess coverage.
>
> How will the Company disclose the costs related to this incident in its financial statements and public filings?
>
> The Company expects it will separately disclose costs specifically related to this incident, as well as any corresponding insurance reimbursements. The timing of recognition of related costs may differ from the timing of recognition of any insurance reimbursement.
>
> What will be the impact to the Company's long-term financial health from this incident?
>
> The Company does not believe this incident will impact its long-term financial health. As a manager and franchisor of leading lodging brands, the Company generates meaningful cash flow each year with only modest capital investment needed to grow the business. The Company remains committed to maintaining its investment grade credit rating.

415. Following Marriott's November 30, 2018 disclosure of the 2014 Starwood data breach, on November 30, 2018 *CNBC* published an article titled "The Marriott hack that stole data

from 500 million people started four years ago — investors should ask how the company missed it" which stated in relevant part (and posed the questions which are central to this action):

> The Marriott breach has the sheer numbers and brand star power to make people take notice: 500 million people were affected, including possibly anyone who stayed at ubiquitous Marriott and Starwood properties across the globe. An unknown attacker stole information including emails, names, addresses, passport numbers and possibly payment card information, in a slow-moving attack that lasted four years.
>
> The breach itself isn't terribly unusual except for two critical questions:
>
> ***Why did its security systems fail to detect a breach until four years after it started?***
>
> ***Did a huge merger between Marriott and Starwood in 2016 lead either company to lose full sight of its corporate-wide technology and security risk?***
>
> * * *
>
> Most details of the breach are still unclear and pending investigation, the company said. The company said it was investigating all aspects of the attack, including how it occurred, whether unencrypted payment data was accessed or why a security tripwire wasn't activated when the thefts began in 2014, among other details.
>
> But customers and investors may have deeper concerns about the time it took to detect the breach and what it means for the companies' existing security investments.
>
> Like most large companies that deal with sensitive financial data, Marriott has a sophisticated cybersecurity program with access to top-line security vendors and tools. Having a single breach, apparently from one origin, slide under the radar for four years is a big deal. Marriott will almost certainly do an internal review to find out which products failed and how.
>
> ***The event***, which the company said affected the Starwood guest reservation database, ***may also call into question how the company conducted cybersecurity due diligence prior to its merger with the rival chain***. The 2016 merger brought the W Hotel, Sheraton and St. Regis brands into the Marriott fold. [Emphasis added]

416. Also, on November 30, 2018 various news agencies published articles about the 2014 Starwood data breach, which included various security experts' reactions. For example:

(a) *Chicago Tribune*[20] – "'On a scale of 1 to 10 and up, this is one of those No. 10 size breaches. There have only been a few of them of this scale and scope in the last decade,' said Chris Wysopal, chief technology officer of Veracode, a security company", and "Security analysts were especially alarmed to learn that the breach began in 2014. 'While such failures often span months, four years is extreme', said Yonatan Striem-Amit, chief technology officer of Cybereason."

(b) *Associated Press*[21] – "'It's an extraordinary breach at a variety of levels,' said Suni Munshani, CEO of Stamford-based data-security firm Protegrity. 'All of this easily could have been prevented. None of this data should have been left unsure and in the open, where somebody could steal it and leverage it.'"

(c) *Washington Post* – "[The] breach of the reservation system for Marriott's Starwood subsidiaries was one of the largest in history… and was particularly troubling for the nature of the data that was apparently stolen."

(d) *Krebs on Security* – The Breach was "a massive data breach exposing the personal and financial information of as many as a half billion customers who made reservations at [] Starwood['s] properties over the past four years," and was "just the latest in a long string of intrusions involving credit card data stolen from major hotel chains over the past four years."

(e) *New York Times* – "[P]rivacy advocates said there was no excuse for a breach to go unnoticed for four years."

417. In response to this news, shares in Marriott's stock fell $6.81 or over 5.5% to close

[20] *See* Footnote 11.

[21] *See Associated Press* article titled "Starwood hit by cyber breach" at https://www.apnews.com/6a8631a9bd314f2b8a988784b6358c60 (Last visited Aug. 4, 2020).

at $115.03 per share on November 30, 2018, damaging investors.

418. On December 3, 2018, Senators John Thune, Roger F. Wicker and Jerry Moran sent a letter to Defendant Sorenson seeking additional information regarding the data breach by no later than 5:00 P.M on December 17, 2018. Information requested includes the time at which the Company became aware of information relevant to the investigation, whether payment card information was encrypted using the AES-128 standard, and how non-payment information was secured and encrypted.

419. On December 4, 2018, the *Los Angeles Times* published a story reporting that, following the data breach, Marriott has agreed to pay for passport replacements if it finds that customers have been victims of fraud. The article stated, in relevant part:

> After a colossal data breach that hit Marriott International and compromised sensitive personal information — including some passport numbers — of hundreds of millions of guests, the hotel company has agreed to pay for passport replacements if it finds that customers have been victims of fraud.
>
> ***The breach, which took place over four years and affected 500 million guests***, was notable not only for its scope but also for the bevy of personal information hackers accessed through the reservation system of Marriott's subsidiary, Starwood: genders, birth dates, email and mailing addresses and phone numbers, as well as some payment card information. The hackers also accessed passport numbers for a "smaller subset of customers," Marriott said.
>
> The U.S. State Department has said that its records and systems were not connected to Marriott's and that a fake passport could not be created with a passport number alone.
>
> But many experts and government officials have expressed concern that the passport numbers, in concert with the other personal data compromised by the hack, could pose serious risks of identity theft — and be a threat to national security.

420. The article continued, stating:

> On Sunday, Senate Minority Leader Chuck Schumer (D-N.Y.) suggested that Marriott cover the $110 charge for customers requesting new passports after the breach.
>
> Marriott spokeswoman Connie Kim said in an email that although it believes the

> chance of hackers using passport numbers "is very low," the hotel giant is willing to foot the bill in cases it deems necessary.
>
> "We are setting up a process to work with our guests who believe that they have experienced fraud as a result of their passports being involved in this incident," Kim said. "If, through that process, we determine that fraud has taken place, then the company will reimburse guests for the costs associated with getting a new passport."

421. Regarding the scope of the Data Breach, the *Los Angeles Times* reported:

> ***Hackers accessed the reservation system of Starwood hotels*** — which includes the Sheraton, St. Regis and Westin brands, among others — ***sometime in 2014. The breach went undetected during Marriott's acquisition of Starwood in 2016 and wasn't discovered until early September of this year***. After Marriott announced the hacking attack Friday, the hotel giant was deluged with criticism about its security practices and with questions about what it was doing to protect its customers.
>
> ***New York Atty. Gen. Barbara Underwood, Maryland Atty. Gen. Brian Frosh and Pennsylvania Atty. Gen. Josh Shapiro all said their offices had opened investigations into the Marriott breach***. And for many other government officials, the breach has become a rallying cry for arguing for stricter consumer privacy regulation. [Emphasis added.]

422. On December 5, 2018, Defendant Oberg stated that as a result of the Data Breach, Marriott "had an ongoing data security program for a while," and that Marriott "had a plan" but "as a result of [the Breach], we're stepping it up even faster." That same day, C/Net reported that "[i]nvestigators believe there may have been more than one hacking group inside the guest reservation network for Marriot's Starwood division at the same time. This could make it harder to identify the culprit, as one of the sources noted." On December 6, 2018, *USA Today* also reported that the Company had agreed to "pay for customer's new passports if they can prove fraud following the company's large-scale data breach."

423. On December 18, 2018, 102 days after Marriott discovered the Data Breach, Marriott stopped operating Starwood's corrupted guest reservation database.

424. Cybersecurity experts have criticized the Company's response to the data breach. A December 3, 2018 article published by *TechCrunch* noted that the notification sent to customers

whose PII may have been compromised appeared illegitimate, and the Company's response left customer's vulnerable to scammers attempting to spoof messages from the Company. Such response failures further diminish the Company's reputation and undermine consumer's trust in its brand.

425. On March 4, 2019 Defendants caused Marriott to publish updated information regarding the Data Breach. In this Update, Marriott stated in relevant part:

> After further data analysis we have identified approximately 383 million records as the upper boundary for the total number of guest records that were involved in the incident. This does not, however, mean that information about 383 million unique guests was involved, as in many instances, there appear to be multiple records for the same guest. We concluded with a fair degree of certainty that information for fewer than 383 million unique guests was involved, although the company is not able to quantify that lower number because of the nature of the data in the database.
>
> Allowing for the fact that even the most exhaustive investigation cannot necessarily provide complete certainty, Marriott now believes the following about the data involved in the incident:
>
> There were approximately 9.1 million unique encrypted payment card numbers, approximately 385,000 of which cards were unexpired as of September 2018; and
>
> There were approximately 5.25 million unique unencrypted passport numbers and approximately 18.5 million encrypted passport numbers.
>
> Certain data analytics work continues, but based on preliminary information, we believe that the data involved in the incident could also include several thousand unencrypted payment card numbers.

426. On March 7, 2019, Defendant Sorenson testified before the Senate Permanent Subcommittee on Investigations. During the hearing, Senator Tom Carper questioned Marriott's data security policies, stating that "Marriott acquired a company that it knew had serious cybersecurity challenges and had actually been attacked before," yet "chose to initially leave Starwood's security system in place after acquiring the company.

## XII. REPURCHASES OF COMPANY STOCK DURING THE RELEVANT PERIOD

427. During the period in which the Company made false and misleading statements and omissions, Defendants caused the Company to initiate repurchases of its common stock at artificially inflated prices that substantially damaged the Company. In total, the Company spent an aggregate amount of approximately $3.39 billion to repurchase approximately 26 million shares of its own stock from October 2017 through September 2018.

428. As the Company stock was actually only worth $113.50 per share, the price at closing on December 4, 2018, the Company overpaid more than $451.4 million in total for these repurchases.

429. According to the Company's 2017 Form 10-K, in the month of October 2017, Defendants caused the Company to repurchase 2.1 million shares of its own common stock at an average price per share of approximately $115.65, for a total cost to the Company of approximately $242.9 million.

430. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $2.15 more than the actual worth of each share during the month of October 2017. Thus, the total over payment by the Company for repurchases of its own stock during October 2017 was over $4.5 million.

431. According to the Company's 2017 Form 10-K, in the month of November 2017, Defendants caused the Company to repurchase 2.0 million shares of its own common stock at an average price per share of approximately $124.30, for a total cost to the Company of $248.6 million.

432. Due to the artificial inflation of the Company's stock price caused by

misrepresentations alleged to have been made by Defendants, the Company paid on average $10.80 more than the actual worth of each share during the month of November 2017. Thus, the total over payment by the Company for repurchases of its own stock during November 2017 was $21.6 million.

433. According to the Company's 2017 Form 10-K, in the month of December 2017, Defendants caused the Company to repurchase 3.3 million shares of its own common stock at an average price per share of approximately $131.20, for a total cost to the Company of approximately $433 million.

434. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $17.70 more than the actual worth of each share during the month of December 2017. Thus, the total over payment by the Company for repurchases of its own stock during December 2017 was over $58.4 million.

435. According to the Company's Form 10-Q for the fiscal quarter ended March 31, 2018, filed with the SEC on May 10, 2018 (the "Q1 2018 10-Q"), in the month of January 2018, Defendant caused the Company to repurchase 1.7 million shares of its own common stock at an average price per share of approximately $139.82, for a total cost to the Company of approximately $237.7 million.

436. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $26.32 more than the actual worth of each share during the month of January 2018. Thus, the total over payment by the Company for repurchases of its own stock during January 2018 was over $44.7 million.

437. According to the Company's Q1 2018 10-Q, in the month of February 2018, Defendants caused the Company to repurchase 1.4 million shares of its own common stock at an average price per share of approximately $139.18, for a total cost to the Company of approximately $194.9 million.

438. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $25.68 more than the actual worth of each share during the month of February 2018. Thus, the total over payment by the Company for repurchases of its own stock during February 2018 was approximately $36 million.

439. According to the Company's Q1 2018 10-Q, in the month of March 2018, Defendants caused the Company to repurchase 2.5 million shares of its own common stock at an average price per share of approximately $138.79, for a total cost to the Company of approximately $347 million.

440. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $25.29 more than the actual worth of each share during the month of March 2018. Thus, the total over payment by the Company for repurchases of its own stock during March 2018 was approximately $63.2 million.

441. According to the Company's Form 10-Q for the fiscal quarter ended June 30, 2018, filed with the SEC on August 7, 2018 (the "Q2 2018 10-Q"), in the month of April 2018, Defendants caused the Company to repurchase 1.5 million shares of its own common stock at an average price per share of approximately $134.62, for a total cost to the Company of approximately $201.9 million.

442. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $21.12 more than the actual worth of each share during the month of April 2018. Thus, the total over payment by the Company for repurchases of its own stock during April 2018 was over $31.7 million.

443. According to the Company's Q2 2018 10-Q, in the month of May 2018, Defendants caused the Company to repurchase 2.6 million shares of its own common stock at an average price per share of approximately $136.78, for a total cost to the Company of over $355.6 million.

444. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $23.28 more than the actual worth of each share during the month of May 2018. Thus, the total over payment by the Company for repurchases of its own stock during May 2018 was over $60.5 million.

445. According to the Company's Q2 2018 10-Q, in the month of June 2018, Defendants caused the Company to repurchase 2.1 million shares of its own common stock at an average price per share of approximately $136.58, for a total cost to the Company of over $286.8 million.

446. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $23.08 more than the actual worth of each share during the month of June 2018. Thus, the total over payment by the Company for repurchases of its own stock during June 2018 was approximately $48.5 million.

447. According to the Company's Q3 2018 10-Q, in the month of July 2018, Defendants caused the Company to repurchase 2.0 million shares of its own common stock at an average price

per share of approximately $129.97, for a total cost to the Company of over $259.9 million.

448. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $16.47 more than the actual worth of each share during the month of July 2018. Thus, the total over payment by the Company for repurchases of its own stock during July 2018 was over $32.9 million.

449. According to the Company's Q3 2018 10-Q, in the month of August 2018, Defendants caused the Company to repurchase 3.4 million shares of its own common stock at an average price per share of approximately $122.85, for a total cost to the Company of approximately $417.7 million.

450. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $9.35 more than the actual worth of each share during the month of August 2018. Thus, the total over payment by the Company for repurchases of its own stock during August 2018 was approximately $31.8 million.

451. According to the Company's Q3 2018 10-Q, in the month of September 2018, Defendants caused the Company to repurchase 1.3 million shares of its own common stock at an average price per share of approximately $127.01, for a total cost to the Company of over $165.1 million.

452. Due to the artificial inflation of the Company's stock price caused by misrepresentations alleged to have been made by Defendants, the Company paid on average $13.51 more than the actual worth of each share during the month of September 2018. Thus, the total over payment by the Company for repurchases of its own stock during September 2018 was

approximately $17.6 million.

453. In total, the Company overpaid an aggregate amount of over $451.4 million for repurchases of its own stock during the period of time in which the Company made false and misleading statements and omissions.

## XIII. LOSS CAUSATION

454. During the Relevant Period, Defendants engaged in a scheme to deceive the market and a course of conduct that artificially inflated the price of Marriott's securities and operated as a fraud or deceit on Relevant Period purchasers of Marriott's securities by failing to disclose and misrepresenting the adverse facts and risks detailed herein. Later, when Defendants prior misrepresentations and fraudulent course of conduct, and/or the information alleged herein to have been concealed from the market, and/or the effects thereof, were revealed to the market, the price of Marriott's securities declined significantly as the prior artificial inflation was released from the Company's share price. Specifically, Defendants materially false and misleading statements, half-truths, and omissions misrepresented, *inter alia*, the extent of Marriott's due diligence when it acquired Starwood, the extreme vulnerability of Starwood's systems, the state of Starwood and Marriott's IT security during the Integration, and Marriott's data security and cybersecurity practices.

455. As a result of the Company's purchases of Marriott's securities during the Relevant Period, the Company suffered economic loss, *i.e.*, damages, under the federal securities laws. The Directors Defendants false and misleading statements, half-truths, and omissions had the intended effect and caused Marriott's securities to trade at artificially inflated levels throughout the Relevant Period, closing as high as $147.99 on January 29, 2018.

456. By concealing from the Company the adverse facts and risks related to the Merger,

Integration, and cybersecurity detailed herein, Defendants presented a misleading picture of Marriott's business and prospects. When the information and/or underlying conditions, and/or effects thereof were revealed to the market through corrective disclosure and/or a materialization of the concealed risk, the price of Marriott's securities fell dramatically. This decline removed the artificial inflation from the price of Marriott's securities, causing economic loss to the Company who had purchased Marriott's securities during the Relevant Period.

457. The decline in the price of Marriott's securities following the corrective disclosure and/or materialization of the concealed risk on November 30, 2018, was a direct result of the nature and extent of Defendants' fraudulent misrepresentations, half-truths, and omissions being revealed to the market. The timing and magnitude of the price declines in Marriott's securities, Defendants' post-Class Period revelations, and analyst reactions to the news negate any inference that the loss suffered by the Company was caused by changed market conditions, macroeconomic or industry factors, unrelated to Defendants' fraudulent conduct.

458. The economic loss, *i.e.*, damages, suffered by the Company was a direct result of Defendants fraudulent scheme and course of conduct to artificially inflate the price of Marriott's securities and the subsequent material decline in the value of Marriott's securities when Defendants' prior misrepresentations, misleading omissions and half-truths, and other fraudulent conduct were revealed.

459. Specifically, on November 30, 2018, Defendants revealed that the legacy Starwood guest reservation database that Marriott owned and operated had been compromised by a breach since at least two years before Marriott acquired it. On November 30, 2018, Defendants revealed that the sensitive, personal information of approximately 500 million guests had been stolen from Marriott's customers through the Data Breach in the legacy Starwood guest reservation database.

Defendants revealed that attackers had stolen: (1) names; (2) passport numbers; (3) dates of birth; (4) credit card information; (5) home addresses; and (6) other valuable, sensitive personal information.

460. As a result of this corrective disclosure and/or revelation of a previously concealed, materialized risk, Marriott's share price dropped by $6.81 from a close of $121.84 per share on November 29, 2018 to $115.03 per share on November 30, 2018, a decline of 5.59%.

461. Several news outlets issued reports discussing the announcement of the Data Breach and resulting share price decline. *MarketWatch* also reported that Marriott's share price dropped "5.6% in premarket trade Friday, after the hotel operator disclosed a 'data security incident' of its Starwood guest reservation database that contains information on up to 500 million guests." Additionally, *Bloomberg* reported that Marriott's share price "tumble[d]" on the revelation of the Data Breach, and Nasdaq.com reported that Marriott's share price "was falling hard" on news of the Data Breach.

462. This share price reaction was the direct result of the market learning facts that Defendants had concealed throughout the Relevant Period, including that throughout the Integration, the legacy Starwood guest reservation system and database had been compromised by the Data Breach and that Starwood's IT systems were severely vulnerable and susceptible to hacking—facts that an adequate due diligence process would have easily revealed. Indeed, this corrective disclosure and/or materialization of a concealed risk revealed to the market that Defendants had made false and misleading statements, half-truths, and omissions throughout the Relevant Period, as detailed in Section IX.

## XIV. APPLICATION OF PRESUMPTION OF RELIANCE

463. The Company is entitled to a presumption of reliance on Defendants' material

misrepresentations and omissions pursuant to the fraud-on-the-market theory:

(a) Marriott's securities were actively traded on the NASDAQ and Chicago Stock Exchange, informationally efficient markets, throughout the Relevant Period;

(b) Marriott's securities traded at high weekly volumes during the Relevant Period;

(c) Defendants filed periodic public reports with the SEC;

(d) Defendants regularly communicated with public investors by means of established market communication mechanisms, including through regular dissemination of press releases on the major news wire services and through other wide-ranging public disclosures, such as communications with the financial press, securities analysts and other similar reporting services;

(e) the market reacted promptly to public information disseminated by Defendants;

(f) Marriott's securities were covered by numerous securities analysts employed by major brokerage firms who wrote reports that were distributed to the sales force and certain customers of their respective firms. Each of these reports was publicly available and entered the public marketplace. The firms who wrote analyst reports on Marriott during the Relevant Period include, but are not limited to, the following: Barclays, Deutsche Bank, JP Morgan, Jefferies, SunTrust Robinson Humphrey, Wells Fargo, and others;

(g) the material misrepresentations and omissions alleged herein would tend to induce a reasonable investor to misjudge the value of Marriott's securities; and

(h) without knowledge of the misrepresented or omitted material facts alleged

herein, the Company purchased shares of Marriott's securities between the time Defendants misrepresented or failed to disclose material facts and the time the true facts were revealed.

464. In the alternative, the Company is entitled to a presumption of reliance under *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the claims asserted herein against the Directors Defendants are primarily predicated upon omissions of material facts which there was a duty to disclose.

## XV. NO SAFE HARBOR

465. The statutory safe harbor provided by the PSLRA for forward-looking statements under certain circumstances does not apply to any of the materially false and misleading statements and omissions alleged herein.

466. First, Defendants statements and omissions alleged to be false and misleading relate to historical facts or existing conditions, and omissions are not protected by the statutory safe harbor. Defendants false and misleading statements and omissions alleged herein are not forward-looking because such statements: (1) relate to historical or current fact; (2) implicate existing conditions; and (3) do not contain projections of future performance or future objective. To the extent that any of the alleged false and misleading statements and omissions might be construed to touch on future intent, they are mixed statements of present facts and future intent and are not entitled to safe harbor protection with respect to the part of the statement that refers to the present.

467. Second, any purported forward-looking statements were not accompanied by meaningful cautionary language because any risks that Defendants warned of had already come to pass, and any cautionary language did not mention important factors of similar significance to those actually realized. Additionally, to the extent Defendants included any cautionary language,

such language was not meaningful because any potential risks identified by Defendants had already manifested. To the extent Defendants included any cautionary language, it was not precise, not meaningful, and did not relate directly to any forward-looking statements at issue. The cautionary language was boilerplate and did not meaningfully change during the Relevant Period, despite the fact that conditions had materially changed.

468. Third, to the extent that there were any forward-looking statements that were identified as such, Defendants are liable because, at the time each of those forward-looking statements were made, the speaker knew the statement was false when made.

## XVI. DAMAGES TO MARRIOTT

469. As a direct and proximate result of Defendants' conduct, Marriott has lost and expended, and will lose and expend, many millions of dollars.

470. Such expenditures include, but are not limited to, legal fees associated with the Securities Class Action pending against the Company, its CEO, CFO, and CAO, and amounts paid to outside lawyers, accountants, and investigators in connection thereto.

471. Such expenditures include, but are not limited to, legal fees associated with the actions in the MDL Action filed against the Company, and amounts paid to outside lawyers, accountants, and investigators in connection thereto.

472. Such expenditures include, but are not limited to, legal fees associated with the investigations into the Company launched by the Attorneys General of the states of Maryland, New York and Georgia, and amounts paid to outside lawyers, security experts, and investigators in connection thereto.

473. Such expenditures include, but are not limited to, the costs of implementing the Response Measures, including WebWatcher enrollment for those affected by the Data Breach.

474. Such expenditures include, but are not limited to, the costs of replacing passports for individuals affected by fraud as a result of the Data reach.

475. Such losses include, but are not limited to, approximately $451.4 million that the Company overpaid, at the direction of Defendants, for its repurchases of its own stock at artificially inflated prices.

476. In addition, these expenditures include, but are not limited to, handsome compensation and benefits paid to Defendants who breached their fiduciary duties to the Company, and benefits paid to Defendants who breached their fiduciary duties to the Company.

477. As a direct and proximate result of Defendants' conduct, Marriott has also suffered and will continue to suffer a loss of reputation and goodwill, and a "liar's discount" that will plague the Company's stock in the future due to the Company's and their misrepresentations and Defendants' breaches of fiduciary duties and unjust enrichment.

478. The fallout from the second largest data breach in history has also included investigations from "certain committees of the U.S. Senate and House of Representatives" and "regulatory authorities in various other jurisdictions." Additionally, approximately 100 lawsuits have been filed against Marriott and Starwood from a variety of plaintiffs, including residents of all fifty states and foreign citizens in American and Canadian courts.

### A. This Court Has Already Determined That Certain Defendants Made Material Omissions About The Company's Due Diligence And Data Security And Knew The Company's Due Diligence And Data Security Were Inadequate

479. This Court has already made several important rulings in parallel proceedings that apply to Plaintiffs' allegations here. The Court held in a decision on the Defendants' motion to dismiss in the parallel Consumer Track, based on substantially the same facts, that plaintiffs met the heightened pleading requirements of Rule 9(b) with regard to: (1) "their allegations of reliance

on material omissions by Defendants." Consumer MTD Opinion at 60-61, 64. ECF 540

480. Additionally, the Court held that the Section 5 of the FTC Act "is a statute that creates enforceable duties," and that duty "is ascertainable as it relates to data breach cases." Consumer MTD Opinion at 47. In discussing the duty imposed on Marriott by Section 5 of the FTC Act, the Court highlighted the Court of Appeals for the Third Circuit's decision in *FTC v. Wyndham* from 2015. *Id.* at 48. The Court noted that the Third Circuit found that "allegations regarding Wyndham's cybersecurity practices, including that it had an allegedly misleading privacy policy that overstated its cybersecurity, fell within the plain meaning of 'unfair' practices in the text of Section 5 of the FTC Act." *Id.* Further, the Court highlighted that the Third Circuit relied in part on the guidance from the FTC titled Protecting Personal Information: A Guide for Business, published in 2007. *Id.* That guide from the FTC "provided additional" notice to Wyndham regarding their data protection duties under Section 5 of the FTC Act. *Id.*

481. On December 13, 2019, the Court denied Defendants' motion to dismiss in the Government Track. ECF No. 517 (Court's Memorandum Opinion and Order on Defendants' Motion to Dismiss Chicago's First Amended Complaint) ("Government MTD Order"). The amended complaint in the Government Track noted that the filing of that action was prompted by a request from the Commissioner for the City of Chicago Department of Business Affairs and Consumer Protection, Rosa Escareno, after she completed her investigation into the Data Breach. Government Complaint at ¶ 10, n.7. As stated in the Government MTD Order: "Chicago alleges that Marriott's data security practices were unfair, deceptive, and unlawful" under a municipal ordinance, and Illinois state statutes. Government MTD Order at 5. In denying Defendants' motion to dismiss, the Court held that Chicago adequately pleaded an injury to the city's proprietary interests in the form of guests being less likely to stay at Marriott hotels in Chicago as

a result of the Data Breach. *Id.* at 6-8.

482. On February 7, 2020, the Court denied Defendants' motion to dismiss, in part, in the Financial Institution Track. ECF No. 532 (Court's Memorandum Opinion and Order on Defendants' Motion to Dismiss Bank of Louisiana's First Amended Complaint) ("Financial Institution MTD Order"). The plaintiffs in the Financial Institution Track alleged that "Marriott chose not to address known and identified security vulnerabilities in Starwood's environment despite concerns from several data security assessors." Financial Institution Complaint at ¶ 12. Additionally, the Financial Institution Track plaintiffs noted that "[m]any of these security deficiencies were the same ones identified by previous security assessments of Starwood's systems and databases," and that "at least some of the PCI DSS violations both 'caused' and 'contributed' to the Data Breach." *Id.* at ¶ 18. Further, the Financial Institution Track's amended complaint, based on its review of the PFI Report, alleged that Marriott committed "numerous violations of the PCI DSS requirements." *Id.* at ¶ 59.

**B. Regulatory Proceedings**

483. In addition to the litigation detailed above, Marriott has also been the subject of regulatory proceedings from various state and federal agencies.

484. As the Company has disclosed at the end of each quarter since revealing the Data Breach, and as of the end of Q4 2020, Marriott has spent approximately $114 million on remedial measures related to the Data Breach. Though most of those costs have been reimbursed by insurance thus far, Marriott has noted in its SEC filings that the Data Breach and similar incidents could make insurance unavailable. Additionally, Marriott is being investigated by the Attorneys General of all fifty states and the District of Columbia, the FTC, and the SEC. Further, on July 9, 2019, the ICO announced its intention to fine Marriott more than $120 million for failure to comply

with GDPR. The ICO's investigation "found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems." In the Company's response to the ICO's investigation into the Data Breach, Marriott claimed that it "had no reason to conclude that the [Merger] was likely to result in a high risk" that data would be compromised, Consumer Complaint at ¶ 219, which could not have been further from the truth. Marriott also admitted that it did not conduct "any formal data protection impact assessment in relation to its acquisition of Starwood." *Id.* According to the ICO, a data protection impact assessment ("DPIA") is a process that helps companies identify and minimize the data protection risks related to a project. A company is required to conduct a DPIA when data processing is likely to result in a high risk to individuals. The ICO will consider comments from EU residents who were affected by the Data Breach, and Marriott before making a final ruling on the fine, currently scheduled for September 2020.

## XVII. DERIVATIVE ALLEGATIONS

485. Plaintiffs incorporate by reference and re-alleges each and every allegation stated above as if fully set forth herein.

486. Plaintiffs bring this action derivatively in the right and for the benefit of the Company to redress injuries suffered and to be suffered as a direct and proximate result of the breaches of fiduciary duties by Defendants.

487. Plaintiffs will adequately and fairly represent the interests of the Company and its shareholders in enforcing and prosecuting its rights and has retained counsel competent and experienced in derivative litigation.

488. Plaintiffs are current owners of Marriott stock. Plaintiffs understand their obligation to hold stock throughout the duration of this action and are prepared to do so.

## XVIII. DEMAND FUTILITY ALLEGATIONS

489. During the wrongful course of conduct at the Company, the Board consisted of the Director Defendants. Because of the facts set forth throughout this Complaint, demand on the Board to institute this action is not necessary because such a demand would have been a futile and useless act.

490. The Marriott Board is presently comprised of eleven (11) members – Defendants JW Marriott, Harrison, Henderson, Hippeau, Kellner, Lee, Lewis, Muñoz, Schwab, Sorenson, and non-party Margaret M. McCarthy ("Demand Director Defendants"). Thus, Plaintiffs are required to show that a majority of the Demand Director Defendants, *i.e.*, six (6), cannot exercise independent objective judgment about whether to bring this action or whether to vigorously prosecute this action.

491. These defendants either knew or should have known of the false and misleading statements that were issued on the Company's behalf and took no steps in a good faith effort to prevent or remedy that situation. Each of these defendants authorized and/or permitted the false statements to be disseminated directly to the public and made available and distributed to shareholders, and are principal beneficiaries of the wrongdoing alleged herein, and thus, could not fairly and fully prosecute such a suit even if they instituted it.

492. The Director Defendants, in particular, Defendant Sorenson, like Defendant Oberg and other Marriott executives publicly emphasized the significance of customer data to both the Merger and to Marriott's business operations in general. These defendants were well aware at all relevant times that the Company's customers and its reservation systems comprised core components of Marriott's operations. Moreover, many of Marriott's partnerships were premised on shared customer information. As such, due diligence processes concerning the Company's and

Starwood's guest reservation databases during the pre-merger and post-merger periods should have been primary focuses for the Director Defendants. The Merger was a significant transaction worth at least $13 billion—the largest acquisition of Marriott's to date. A primary component of the Merger was, after all, Starwood's customer data. Therefore, the success of the Merger depended on the successful and secure integration of both companies' systems. As alleged herein, the Director Defendants failed to adequately exercise due diligence in connection with the Merger in order to timely identify and address glaring weaknesses in Starwood's system. The Director Defendants failed to uncover and mitigate these vulnerabilities in an appropriate and timely manner, despite having countless opportunities over several years.

493. Significantly, according to the Securities Complaint, and upon information and belief, CW 5, a Senior Director at the Company during the Relevant Period, stated that Starwood's antiquated Oracle system was beyond repair—as it would have cost Starwood hundreds of millions to fix. According to CW 5 this was Starwood's main reason for agreeing to the merger with Marriott. CW 5 maintained that the Company was aware of this. Furthermore, according to the Securities Complaint, and upon information and belief, CW 1 stated that the vast majority of decisions at Marriott concerning data security were decided based on financial expenditure. Such decisions therefore would have fallen within the purview of the Board in order to gain approval of budget plans. The Board therefore would have been aware that the budget they approved could not have accounted for the necessary upgrades to Starwood's systems.

494. The Director Defendants were responsible for risk oversight, including reviewing the Company's cybersecurity risk profile. The Director Defendants were informed on the specifics of the cybersecurity risk program in a separate annual presentation by the Company's Chief Information Officer, and is further briefed on actions and changes taken by management to

mitigate the Company's risk profile and provided with an overview of the cybersecurity strategy along with key cybersecurity initiatives and incidents. As a result of such disclosures to the Board, the Director Defendants were provided with an overview of the cybersecurity risks and threats landscape. According to the 2018 Proxy Statement, the Director Defendants used such information to review the Company's risk posture. As a result of this knowledge, the Director Defendants, were, or should have been aware, of the cybersecurity risks posed by its failure to securely store the personal information of its customers. As a result, the Director Defendants face a substantial likelihood of liability, and therefore, demand is excused.

495. Further, at the time of the Merger, Starwood had publicly announced that it had experienced a cybersecurity incident. In light of the Board's duties of oversight with respect to the Merger, and the risk oversight duties outlined in the 2018 Proxy Statement, the Director Defendants, with the exception of Defendants Duncan, Hippeau, and Lewis, breached their duty of oversight by allowing the Merger to go forward without conducting adequate due diligence to discover the ongoing Data Breach, especially in light of the known 2015 Starwood Data Breach and the significant data breaches plaguing Marriott's competitors and other industries involving sensitive customer information. As a result, the Director Defendants, with the exception of Defendants Duncan, Hippeau, and Lewis, face a substantial likelihood of liability due to this failure of oversight, and therefore, demand is excused.

496. Moreover, prevalent red flags described herein support that the Director Defendants knew or were reckless for not knowing the gravity of Marriott's due diligence in connection with the Merger. Yet, in breach of their responsibilities, they allowed Marriott to merge with a company that operated with flagrantly unsecured IT systems and moreover failed to ensure proper scans were being implemented that would have timely identified the prevalent vulnerabilities.

497. In complete abdication of their fiduciary duties, the Director Defendants either knowingly or recklessly participated in the conduct alleged herein. The fraudulent scheme was, *inter alia*, intended to make the Company appear more stable, profitable, and attractive to investors.

498. As a result of the foregoing, the Director Defendants breached their fiduciary duties, face a substantial likelihood of liability, are not disinterested, and demand upon them is futile, and thus excused.

499. As more fully discussed below, a majority of the Director Defendants, *i.e.*, at least six (6), cannot exercise independent objective judgment about whether to bring this action or whether to vigorously prosecute this action:

**A. Defendant Sorenson**

500. Defendant Sorenson is not disinterested or independent, and therefore, is incapable of considering demand because he (as its President and CEO) is an employee of the Company who derives substantially all his income from his employment with Marriott, making him not independent. As such, Defendant Sorenson cannot independently consider any demand to sue himself for breaching his fiduciary duties to Marriott, because that would expose him to liability and threaten his livelihood. Marriott paid Defendant Sorenson the following compensation:

| Fiscal Year | Salary | Bonus | Stock Awards | SAR Awards | Non-Equity Incentive Plan Compensation | Value and Nonqualified Deferred Compensation Earnings | All Other Compensation | Total |
|---|---|---|---|---|---|---|---|---|
| 2018 | $1,300,000 | -- | $6,222,315 | $2,207,473 | $2,925,000 | $23,309 | $255,895 | $12,933,992 |
| 2017 | $1,300,000 | $1,000,000 | $5,310,583 | $1,838,959 | $3,628,950 | $45,635 | $187,490 | $13,311,617 |
| 2016 | $1,236,000 | --- | $6,010,081 | $2,000,062 | $2,756,527 | $90,184 | $205,524 | $12,298,378 |
| 2015 | $1,236,000 | | $3,830,311 | 2,000,036 | $3,626,919 | $75,740 | $206,411 | $10,975,417 |

501. Defendant Sorenson is also a defendant in the Securities Class Action and faces a substantial likelihood of liability.

502. Further, Marriott admits that Defendant Sorenson is not independent in its 2018 Proxy.

503. As a trusted Company director and CEO during the Relevant Period, Defendant Sorensen knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact (*see* Section VII.G.), consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets.

504. Defendant Sorensen was ultimately responsible for all of the misconduct alleged herein, including the false and misleading statements and omissions that were made (*see* Section IX), including those contained in the Company's SEC filings (*see* Section IX), and the Company's press releases in earnings calls (*see* Section IX), in which he personally made statements. He also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions, as alleged above. *See* Section X. In addition, Defendant Sorensen's own March 7, 2019 congressional testimony confirms that he was aware of the Data Breach from at least September 17, 2018. Nevertheless, he continued to make and/or caused the Company to make statements misrepresenting cyberattacks as mere potential risks as opposed to realized risks and promoting Marriott's integration process while knowing that a fundamental aspect of that process had been impacted by one of the largest data breaches in history.

505. Defendant Sorensen was not a bystander in the Company's mergers and acquisition ("M&A") activities. Indeed, Defendant Sorensen had a history of involvement in M&A work as a partner with Latham & Watkins prior to joining the Company. Defendant Sorensen joined Marriott to work in M&As as early as 1996. He served as an informant for the rest of the Board.

*See* Section VII.B.(4).

506. For these reasons, Defendant Sorensen breached his fiduciary duties, faces a substantial likelihood of liability, is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

**B. Defendant JW Marriott**

507. Defendant JW Marriott is not disinterested or independent, and therefore, is incapable of considering demand because he (as its Executive Chairman) is an employee of the Company who derives substantially all his income from his employment with Marriott, making him not independent. As such, Defendant JW Marriott cannot independently consider any demand to sue himself for breaching his fiduciary duties to Marriott, because that would expose him to liability and threaten his livelihood.

508. Further, Marriott admits that Defendant JW Marriott is not independent in its 2018 Proxy.

509. As a long-time Company director and the Company's Chairman and Executive Chairman, Defendant JW Marriott knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets. Moreover, Defendant JW Marriott was the maker of many of the false statements and omissions of material fact that are alleged herein, as he signed the 2015 Form 10-K, 2016 10-K and 2017 10-K. *See* Section IX. Defendant JW Marriott also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

510. Further, Defendant JW Marriott is the father of Defendant Harrison and son of JW Marriott, Sr., the founder of Marriott. Given their roles and ties to the Company, Defendants JW Marriott and Harrison are not considered "Independent Directors" by the Company. Demand is therefore futile as to Defendants JW Marriott and Harrison.

**C. Defendant Harrison**

511. Defendant Harrison is not disinterested or independent, and therefore, is incapable of considering demand because she (as its Global Officer, Marriott Culture and Business Councils) is an employee of the Company who derives substantially all her income from her employment with Marriott, making her not independent. In fact, Defendant Harrison has held various executive offices with Marriott since 2006 and has otherwise been employed by Marriott since 1975.

512. Further, Marriott admits that Defendant Harrison is not independent in its 2018 Proxy.

513. As a trusted Company director and Company executive, Defendant Harrison knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded her duties to monitor engagement in the scheme, and consciously disregarded her duties to protect corporate assets.

514. Defendant Harrison was the maker of many of the false statements and omissions of material fact that are alleged herein, as she signed the 2015 Form 10-K, 2016 Form 10-K and 2017 Form 10-K. *See* Section IX. Defendant Harrison also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

515. As discussed herein, Defendant Harrison is the daughter of Defendant JW Marriott

and is beholden to Defendant JW Marriott by virtue of their family relationship, and therefore, is unable to evaluate a demand with independence. As reported by the *Washingtonian*, Defendant Harrison assumed her seat on the Board following the ouster of her brother, John W. Marriott III, from the family and business by Defendant JW Marriott, as alleged in a lawsuit filed by John W. Marriott III.

516. For these reasons, Defendant Harrison is not independent or disinterested, and thus demand upon her is futile and, therefore, excused.

**D. Defendant Hippeau**

517. As a trusted Company director, Defendant Hippeau knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets. Moreover, he was the maker of many of the false statements and omissions of material fact that are alleged herein, as he signed the 2016 Form 10-K and 2017 Form 10-K. *See* Section IX. Defendant Hippeau also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

518. Defendant Hippeau also served as a director of Starwood prior to the Acquisition. Defendant Hippeau thus had even more intimate knowledge of Starwood's wholly deficient data security practices and IT system vulnerabilities. Nonetheless, Defendant Hippeau allowed the Company to continue using Starwood's systems. In fact, even after discovering the Data Breach that exposed the private data of approximately 500 million Starwood customers to third-party attackers, the Board failed to discontinue Marriott's use of the legacy Starwood guest reservation

system. Furthermore, Defendant Hippeau served on the board of directors of Starwood from 2013 until the Acquisition in September 2016. While Starwood was under his watch, attackers infiltrated Starwood's IT systems beginning in 2014 and stole the sensitive personal information of hundreds of millions of Starwood customers.

519. Further, as a Starwood director when Marriott acquired that company, Defendant Hippeau received compensation as part of the Acquisition. Accordingly, Defendant Hippeau is unable to consider a demand with respect to the subject matter of the Board overpaying for Starwood.

520. For these reasons, Defendant Hippeau is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

**E. Defendant Lewis**

521. As a trusted Company director and member of the Audit Committee, Defendant Lewis knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets. Moreover, Defendant Lewis was the maker of many of the false statements and omissions of material fact that are alleged herein, as he signed the 2016 Form 10-K and 2017 Form 10-K. *See* Section IX. Defendant Lewis also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

522. Defendant Lewis also served as a director of Starwood prior to the Acquisition. Defendant Lewis thus had even more intimate knowledge of Starwood's wholly deficient data security practices and IT system vulnerabilities. Nonetheless, Defendant Lewis allowed the

Company to continue using Starwood's systems. In fact, even after discovering the Data Breach that exposed the private data of approximately 500 million Starwood customers to third-party attackers, the Board failed to discontinue Marriott's use of the legacy Starwood guest reservation system. Furthermore, Defendant Lewis served on the board of directors of Starwood from 1999 until the Acquisition in September 2016. While Starwood was under his watch, attackers infiltrated Starwood's IT systems beginning in 2014 and stole the sensitive personal information of hundreds of millions of Starwood customers.

523. Further, as a Starwood director when Marriott acquired that company, Defendant Lewis received compensation as part of the Acquisition. Accordingly, Defendant Lewis is unable to consider a demand with respect to the subject matter of the Board overpaying for Starwood.

524. For these reasons, Defendant Lewis is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

**F. Defendant Muñoz**

525. As a long-time Company director and member of the Audit Committee, Defendant Muñoz knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets. Moreover, Defendant Muñoz was the maker of many of the false statements and omissions of material fact that are alleged herein, as he signed the 2015 Form 10-K, 2016 10-K and 2017 10-K. *See* Section IX. Defendant Muñoz also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

526. For these reasons, Defendant Muñoz is not independent or disinterested, and thus

demand upon him is futile and, therefore, excused.

**G. Defendant Henderson**

527. As a trusted Company director and Chair of the Audit Committee, Defendant Henderson knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets. Moreover, Defendant Henderson was the maker of many of the false statements and omissions of material fact that are alleged herein, as he signed the 2016 10-K and 2017 10-K. *See* Section IX. Defendant Henderson also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

528. For these reasons, Defendant Henderson is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

**H. Defendant Kellner**

529. As a long-time Company director and a member of the Audit Committee, Defendant Kellner knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded his duties to monitor engagement in the scheme, and consciously disregarded his duties to protect corporate assets. Moreover, Defendant Kellner was the maker of many of the false statements and omissions of material fact that are alleged herein, as he signed the 2015 Form 10-K, 2016 10-K and 2017 10-K. *See* Section IX. Defendant Kellner also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X.

530. For these reasons, Defendant Kellner is not independent or disinterested, and thus demand upon him is futile and, therefore, excused.

**I. Defendant Lee**

531. As a long-time Company director, Defendant Lee knowingly or recklessly disregarded red flags (*see* Section VII.E.), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded her duties to monitor engagement in the scheme, and consciously disregarded her duties to protect corporate assets. Moreover, Defendant Lee was the maker of many of the false statements and omissions of material fact that are alleged herein, as she signed the 2015 Form 10-K, 2016 Form 10-K and 2017 Form 10-K. *See* Section IX. Defendant Lee also solicited the 2017 Proxy Statement and 2018 Proxy Statement, which contained material misrepresentations and omissions. *See* Section X

532. For these reasons, Defendant Lee is not independent or disinterested, and thus demand upon her is futile and, therefore, excused.

**J. Defendant Schwab**

533. As a trusted Company director and member of the Compensation Policy Committee, Defendant Schwab knowingly or recklessly disregarded red flags (*see* Section VII.E), conducted little, if any, oversight of the Company's engagement in the scheme to make false and misleading statements and/or omissions of material fact, consciously disregarded her duties to monitor engagement in the scheme, and consciously disregarded her duties to protect corporate assets. Moreover, Defendant Schwab was the maker of many of the false statements and omissions of material fact that are alleged herein, as she signed the 2015 Form 10-K, 2016 10-K and 2017 10-K. *See* Section IX. Defendant Schwab also solicited the 2017 Proxy Statement and 2018 Proxy

Statement, which contained material misrepresentations and omissions, as alleged above. *See* Section X.

534. For these reasons, Defendant Schwab is not independent or disinterested, and thus demand upon her is futile and, therefore, excused.

**K. Defendants Bush, Duncan, Henderson, Lewis, Kellner, and Muñoz**

535. During the Relevant Period, Defendants Bush, Duncan, Henderson, Lewis, Kellner and Muñoz (the "Audit Committee Defendants") served as members of the Company's Audit Committee.[22]

536. During 2015, 2016, and 2017, the Audit Committee's responsibilities included: (1) overseeing the Company's accounting, reporting, and financial practices, including the integrity of the financial statements; (2) overseeing the Company's internal control environment and compliance with legal and regulatory requirements; (3) appointing, retaining, overseeing, and determining the compensation for and terms of the agreement with the Company's independent auditor; and (4) overseeing the Company's internal audit function and the internal auditor. At the start of 2018, in addition to the responsibilities just listed, the Audit Committee was also tasked with "[a]ssisting the Board in overseeing and monitoring the Company's information security and data privacy practices." According to Marriott's Annual Proxies in each of 2015, 2016, 2017, and 2018: "There is unrestricted access between the Audit Committee and the independent auditor and internal auditors." In the Audit Committee Charter during the Relevant Period, the Audit

[22] As noted above, the composition of the Audit Committee changed during Relevant Period. From the start of the Relevant Period until September 23, 2016, the defined term Audit Committee Defendants includes Defendants Bush, Henderson, and Kellner. From September 23, 2016 through the present, the defined term Audit Committee Defendants refers to Defendants Henderson, Lewis, and Muñoz. Defendant Bush did not stand for reelection to the Board at the Company's May 8, 2020 annual stockholders meeting but was a member of the Audit Committee from start of the Relevant Period until her departure from the Company.

Committee was required to "periodically review and discuss the Company's business and financial risk management and risk assessment policies and procedures with senior management, the Independent Auditor, and the Chief Audit Executive."

537. In February 2017, the Audit Committee was specifically warned that it needed to "assume a more formal role for cyber oversight. The Audit Committee did not do so. In the year-long period following this warning, the Audit Committee failed to even discuss cybersecurity, much less address the critical deficiencies in the Company's information security systems.

538. The Audit Committee Defendants breached their fiduciary duties of due care, loyalty, and good faith, because the Audit Committee Defendants, *inter alia*, knowingly or recklessly disregarded red flags (*see* Section VII.E.), allowed or permitted false and misleading statements to be disseminated by the Company as alleged herein (*see* Section IX), and otherwise failed to ensure that adequate internal controls were in place regarding the serious business reporting issues and deficiencies described above. Additionally, the Audit Committee Defendants failed to oversee and ensure adequate cybersecurity due diligence prior to Marriott's merger with Starwood.

539. Based thereon and for other reasons described herein, Defendants Bush, Duncan, Henderson, Lewis, and Muñoz face a substantial likelihood of liability for their breach of fiduciary duties and any demand upon them is futile.

### L. Defendants Henderson, Kellner, Lee and Reinemund

540. During the Relevant Period, Director Defendants Kellner, Lee and Reinemund served as members of the Nominating and Corporate Governance Committee (on information and belief, Defendant Henderson joined the Nominating and Corporate Governance Committee sometime in 2018). Pursuant to the Company's Nominating and Corporate Governance

Committee Charter, the members of the Nominating and Corporate Governance Committee are responsible for, *inter alia*, developing corporate governance principles and reviewing the principles on a regular basis for necessary changes, making recommendations regarding the effective functioning of the Board such as the quality, quantity and timeliness of information furnished to Directors, and otherwise meet their responsibilities as set forth in the Nominating and Corporate Governance Committee Charter as set forth herein.

541. Defendants Henderson, Kellner, Lee and Reinemund breached their fiduciary duties by failing to develop and/or implement adequate corporate governance principles and further failed to ensure that the Board was effectively functioning as evidenced by the conduct alleged herein.

542. Based upon the foregoing and other facts contained herein, Defendants Henderson, Kellner, Lee and Reinemund face a substantial likelihood of liability for their breach of fiduciary duties and any demand upon them is futile.

### M. Defendants JW Marriott, Sorenson, Harrison, Henderson, Kellner, Lee, Muñoz, Reinemund, Schwab, and Bush

543. Defendants JW Marriott, Sorenson, Harrison, Henderson, Kellner, Lee, Muñoz, Reinemund, Schwab, and Bush (the "Legacy Marriott Defendants"), were all on the Board at the time that the Merger was approved and at the time that it was consummated and have continuously remained on the Board.

544. The Legacy Marriott Defendants failed to exercise their duty of oversight in reviewing and approving the Merger due to their failure to discover the Data Breach and/or weaknesses in Starwood's IT systems. As a result of this failure of oversight, the Company acquired Starwood, at an artificially inflated price, thus assuming the legal, reputational and financial consequences of the Data Breach.

545. The Legacy Marriott Defendants also had substantial experience with Company acquisitions and the complexity and risks associated with IT (and other) post-merger integration. Notwithstanding that experience and the red flags (*see* Section VII.E.) discussed herein, knowingly or recklessly disregarded their experience and the red flags resulting in the failure to timely identify the Data Breach, permitting the false and misleading statements, and other wrongful conduct alleged herein. *See* Sections IX and X.

546. The Directors may also be protected against personal liability for their acts of mismanagement and breaches of fiduciary duty alleged herein by directors' and officers' liability insurance if they caused the Company to purchase it for their protection with corporate funds, i.e., monies belonging to the stockholders of Marriott. If there is a directors' and officers' liability insurance policy covering the Directors, it may contain provisions that eliminate coverage for any action brought directly by the Company against the Directors, known as, inter alia, the "insured-versus-insured exclusion." As a result, if the Directors were to sue themselves or certain of the officers of Marriott, there would be no directors' and officers' insurance protection. Accordingly, the Directors cannot be expected to bring such a suit. On the other hand, if the suit is brought derivatively, as this action is brought, such insurance coverage, if such an insurance policy exists, will provide a basis for the Company to effectuate a recovery. Thus, demand on the Directors is futile and, therefore, excused.

547. If there is no directors' and officers' liability insurance, then the Directors will not cause Marriott to sue the Defendants named herein, because, if they did, they would face a large uninsured individual liability. Accordingly, demand is futile in that event, as well.

548. Due to this breach of fiduciary duty, the Legacy Marriott Defendants face a substantial likelihood of liability, are not disinterested in the matters challenged herein, and as a

result, demand on the Legacy Marriott Defendants is futile, and therefore, excused.

**N. Defendants Sorenson, Bush, Henderson, Lewis and Muñoz**

549. Defendants Sorenson, Bush, Henderson, Lewis and Muñoz are defendants in the Securities Class Action and face a substantial likelihood of liability.

550. Any suit by the current directors of Marriott to remedy these wrongs would expose Defendants Sorenson, Bush, Henderson, Lewis, and Muñoz to liability for violations of the federal securities laws in the pending Securities Class Action.

551. Demand is therefore futile as to Defendants Sorenson, Bush, Henderson, Lewis, and Muñoz.

**O. Defendants JW Marriott and Harrison**

552. Defendants JW Marriott and Harrison are beneficial owners and controllers of JWM Family Enterprises, L.P. ("Family Enterprises"). Family Enterprises indirectly holds ownership stakes in 17 hotels operated by subsidiaries of the Company, and Family Enterprises paid approximately $12.9 million in fees and expenses to the Company in 2017. Further, Defendants JW Marriott and Harrison are members of the Marriott family. Numerous members of the Marriott family are employed by the Company in management and senior executive roles. In 2017, five members of the Marriott family received in excess of $120,000 in compensation from the Company, earning aggregate compensation in excess of $6.7 million (over $3.3 million excluding JW Marriott's 2017 compensation). Upon information and belief, other members of the Marriott family were employed by the Company in 2017 in roles earning $120,000 or less.

553. Thus, as a result of their family relationships with numerous individuals employed by the Company, Defendants JW Marriott and Harrison are unable to evaluate a demand with independence, and therefore, demand is excused.

## XIX. CAUSES OF ACTION

### COUNT I

### (Against Defendants for Breach of Fiduciary Duties)

554. Plaintiffs incorporate by reference and re-alleges each and every allegation contained above, as though fully set forth herein.

555. The Director Defendants, as directors of the Company, owed Marriott the highest duty of loyalty. The Director Defendants breached their duty of loyalty by knowingly or recklessly: (1) failing to ensure that Marriott had adequate internal controls, risk management procedures, and other policies in place to ensure compliance with state, federal, and international data protection laws and regulations; (2) failing to undertake cybersecurity and technology due diligence when purchasing Starwood; (3) continuing to operate Starwood's severely deficient guest reservation database for more than two years after the Acquisition closed; (4) concealing the Data Breach that exposed and compromised the personal data of approximately 500 million guests for nearly three months after discovering the Data Breach; (5) making or allowing Marriott to make improper statements in its press releases and SEC public filings; and (6) violating the Company's Guidelines, Code of Conduct, and other duties required of directors as set forth in the Company's corporate governance documents. Accordingly, the Director Defendants breached their duty of loyalty to the Company.

556. The Officer Defendants either knew, were reckless, or were grossly negligent in disregarding the illegal activity of such substantial magnitude and duration. The Officer Defendants breached their fiduciary duties by knowingly, recklessly, or with gross negligence: (1) failing to ensure that Marriott had adequate internal controls, risk management procedures, and other policies in place to ensure compliance with state, federal, and international data protection

laws and regulations; (2) failing to undertake cybersecurity and technology due diligence during the Acquisition; (3) continuing to operate Starwood's severely deficient guest reservation database for more than two years after the Acquisition closed; (4) concealing the Data Breach that exposed and compromised the personal data of approximately 500 million guests for nearly three months after discovering the Data Breach; (5) making or allowing the Company to make improper statements in its press releases and public filings; and (6) violating the Company's Guidelines, Code of Conduct, and other duties required of executives as set forth in the Company's corporate governance documents. Accordingly, the Officer Defendants breached their duties of care and loyalty to the Company.

557. The Audit Committee Defendants breached their fiduciary duty of loyalty by approving the statements described herein which were made during their tenure on the Audit Committee, which they knew or were reckless in not knowing contained improper statements and omissions. The Audit Committee Defendants further breached their fiduciary duties by allowing the Board and management to fail in their legal obligations to comply with state, federal, and international regulations concerning data privacy. The Audit Committee Defendants completely and utterly failed in their duties required by the Audit Committee Charter in effect at the time.

558. Defendants had actual or constructive knowledge of the above misrepresentations and omissions of material facts set forth herein, or acted with reckless disregard for the truth, in that they failed to ascertain and to disclose such facts, even though such facts were available to them.

559. Defendants failed to correct and/or caused the Company to fail to rectify any of the wrongs described herein or correct the false and/or misleading statements and omissions of material fact referenced herein, rendering them personally liable to the Company for breaching

their fiduciary duties.

560. As a direct and proximate result of Defendants' failure to perform their fiduciary obligations, the Company has sustained significant damages. As a result of the misconduct alleged herein, Defendants are liable to the Company.

561. As a direct and proximate result of Defendants' breach of their fiduciary duties, the Company has suffered significant damage alleged herein

**COUNT II**

**(Against Defendants for Waste of Corporate Assets)**

562. Plaintiffs incorporate by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

563. Defendants caused the Company to repurchase shares of its own common stock at artificially inflated prices, thereby wasting the Company's assets.

564. Further, Defendants Reinemund, Hippeau, and Schwab as members of the Compensation Policy Committee caused the Company to waste millions of dollars by approving special supplemental bonuses for the purportedly successful integration of Starwood, despite the fact that the Merger resulted in the Company's exposure to liability and reputational damage as a result of the Data Breach.

565. Defendants, in particular Defendants Sorenson, JW Marriott, Harrison, Henderson, Kellner, Lee, Muñoz, Reinemund, and Schwab caused the Company to waste corporate assets by paying $13.6 billion to acquire Starwood in the Merger, as a result of their failure to discover the Data Breach and adequately discount the purchase price as a result of the Data Breach, which was ongoing at the time of the Merger.

566. The wrongful conduct alleged herein was continuous, connected, and on-going

throughout the Relevant Period. It resulted in continuous, connected, and ongoing harm to the Company.

567. As a result of the misconduct described above, Defendants wasted corporate assets by, *inter alia*: (i) paying excessive compensation, bonuses, and termination payments to certain of its executive officers; (ii) awarding self-interested stock options to certain officers and directors; and (iii) incurring potentially millions of dollars of legal liability and/or legal costs to defend Defendants' unlawful actions.

568. As a result of the foregoing, the Company will incur many millions of dollars of legal liability and/or costs to defend unlawful actions, to engage in internal investigations, and to lose financing from investors and business from future customers who no longer trust the Company and its products.

569. As a result of the waste of corporate assets, Defendants are liable to the Company.

570. Plaintiffs, on behalf of Marriott, have no adequate remedy at law.

**COUNT III**

**(Against the Officer Defendants for Unjust Enrichment)**

571. Plaintiffs incorporate by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

572. By their wrongful acts, violations of law, and false and misleading statements and omissions of material fact that they made and/or caused to be made, the Officer Defendants were unjustly enriched at the expense of, and to the detriment of, Marriott.

573. Defendants received unjustly lucrative bonuses tied to the false and misleading statements, or received bonuses, stock options, or similar compensation from Marriott that was tied to the performance or artificially inflated valuation of Marriott, or received compensation that

was unjust in light of Officer Defendants' bad faith conduct.

574. Defendant Sorenson, Oberg and Bauduin, were unjustly enriched through the award of special supplemental bonuses awarded as a result of their purported "outstanding performance in 2017 regarding the ongoing seamless integration of Starwood" due to the fact that the Integration of Starwood was far from seamless in light of the Data Breach.

575. Plaintiffs, as a shareholders and a representatives of Marriott, seek restitution from the Officer Defendants and seek an order from this Court disgorging all profits—including any performance-based or valuation-based compensation—obtained by the Officer Defendants due to their wrongful conduct.

576. Plaintiffs, on behalf of Marriott, have no adequate remedy at law.

## COUNT IV

### (Against Director Defendants for Violations of Section 10(b) of the Exchange Act and SEC Rule 10b-5)

577. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

578. During the Relevant Period, the following Director Defendants signed the following false and misleading SEC documents (*see* Section IX):

(a) **The Company's 2015 Form 10-K**: Defendants Sorenson[23], JW Marriott, Harrison, Lee, Reinemund, Schwab and Bush, Henderson, Kellner and Muñoz (the Audit Committee members);

(b) **The Company's 2016 Form 10-K**: Defendants Sorenson, JW Marriott, Harrison, Lee, Reinemund, Schwab, Duncan, Hippeau, and Bush, Henderson, Kellner,

[23] Defendant Sorenson signed the Company's false and misleading Form 10-Qs: Q3-2016, Q1-2017, Q2-2017, Q3-2017, Q1-2018, Q2-2018, and Q3-2018.

Lewis and Muñoz (the Audit Committee members);

(c) **The Company's 2017 Form 10-K**: Defendants Sorenson, JW Marriott, Harrison, Lee, Reinemund, Schwab, Duncan, Hippeau, and Bush, Henderson, Kellner, Lewis and Muñoz (the Audit Committee members).

579. During the Relevant Period, Director Defendants disseminated or approved public statements that failed to disclose that Starwood's IT systems were severely vulnerable: (1) the systems were using an outdated Oracle application portal that could not be updated or patched; (2) the legacy Starwood system allowed for insecure remote access; (3) only a fraction of Starwood's firewall activity was being logged, so nobody could adequately monitor for attacks; (4) the legacy Starwood system lacked monitoring and logging of remote access, meaning that there was no record of who was remotely accessing the systems; (5) not all database queries were being logged, so nobody could see if a hacker was accessing Starwood's valuable data without permission; and (6) payment account numbers were being stored without encryption, so sensitive data was easily accessible to attackers. An adequate merger due diligence process would have easily revealed these glaring deficiencies, yet Defendants Sorenson, JW Marriott, Harrison, Lee, Reinemund, Schwab, Duncan, Hippeau, Bush, Henderson, Kellner, Lewis and Muñoz knowingly, or with severe recklessness, failed to share this important information with the market. In addition, throughout the Relevant Period, the legacy Starwood guest reservation database was already compromised by the Data Breach.

580. Further, the statements and omissions made and or approved by Director Defendants gave the market/investors a false impression that Marriott had made adequate preparations and dedicated adequate resources to cybersecurity when, in fact, these Defendants failed to secure Starwood's systems, despite their knowledge of cybersecurity risks. Additionally,

as detailed above in the Board minutes pleaded in Section VII.G., the Board was well aware of the risk that cybersecurity posed to the Company, however, these Defendants ignored multiple red flags that should have caused them to discover the Data Breach (or at least safeguard Starwood's vulnerable client data) including, but not limited to: (1) Starwood's known cybersecurity issues, as detailed in Section VII.B.(3) and E.; (2) significant (and public) intrusions into the systems and databases of the Company's competitors in the hospitality industry, as detailed in Section VII.E.; (3) other significant data breaches in other industries, as detailed in Section VII.E; and (4) the passage and imminent enforcement of the GDPR. *See* Section VII.H.(4).

581. With the price of its common stock trading at artificially inflated prices due to Director Defendants misconduct, these Defendants caused the Company to repurchase millions of dollars of its own stock at artificially inflated prices, damaging Marriott.

582. Director Defendants, as top executives and directors of the Company, are liable as direct participants in the wrongs complained of herein. Through their positions of control and authority as directors and officers of the Company, these Defendants were able to and did control the conduct complained of herein and the content of the public statements disseminated by Marriott. Director Defendants acted with scienter in that they either had actual knowledge of the schemes and the misrepresentations and/or omissions of material facts set forth herein, or acted with reckless disregard for the truth in that they failed to ascertain and to disclose the true facts, even though such facts were available to them. Defendant Sorenson and the Audit Committee Defendants (Bush, Henderson, Kellner, Lewis and Muñoz) received direct briefings regarding the issues described herein (*see* Section VII.B.(3)), and were therefore directly responsible for the schemes set forth herein and for the false and misleading statements and/or omissions disseminated to the public through press releases, conference calls, and filings with the SEC.

583. As such, Director Defendants caused the Company to violate Section 10(b) of the Exchange Act and SEC Rule 10b-5 in that they:

(a) employed devices, schemes, and artifices to defraud; and

(b) made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

**COUNT V**

**(Against the Officer Defendants and the Audit Committee Defendants for Violations of Section 20(a) of the Exchange Act)**

584. Plaintiffs incorporate by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

585. This Count is asserted pursuant to Section 20(a) of the Exchange Act against the Officer Defendants and the Audit Committee Defendants.

586. As alleged above, the Officer Defendants and the Audit Committee Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder by making false and misleading statements in connection with the purchase of Marriott's securities and by participating in a fraudulent scheme and course of business or conduct throughout the Relevant Period. This fraudulent conduct was undertaken with knowledge and scienter of each of the Officer Defendants and the Audit Committee Defendants who knew of or acted with severely reckless disregard for the falsity of their statements and the fraudulent nature of this scheme during the Relevant Period.

587. As set forth above, the Officer Defendants and the Audit Committee Defendants were controlling persons of Marriott during the Relevant Period, due to their senior executive and director positions with the Company and their direct involvement in the Company's day-to-day

operations, as well as their ability to exercise and/or actual exercise of influence and control over the Company's dissemination of information.

588. By virtue of the foregoing, the Officer Defendants and the Audit Committee Defendants each had the power to influence and control, and did influence and control, directly or indirectly, the decision-making of Marriott, including the content of its public statements with respect to the success of the due diligence and Integration process of Starwood, and the effectiveness of its cybersecurity and compliance with industry and regulatory norms, as well as the content of the statements made to the market on those topics.

589. The Officer Defendants and the Audit Committee Defendants acted knowingly and intentionally, or in such a severely reckless manner as to constitute willful fraud and deceit upon the Company who purchased shares of Marriott's securities during the Relevant Period.

590. In ignorance of the false and misleading nature of the Officer Defendants and the Audit Committee Defendants' statements and omissions, and relying directly or indirectly on those statements or upon the integrity of the market prices for shares of Marriott's securities, the Company purchased shares of Marriott's securities at an artificially inflated price during the Relevant Period. But for the fraud, the Company would not have purchased shares of Marriott's securities at artificially inflated prices.

591. As set forth herein, when Defendants subsequently revealed adverse, previously undisclosed facts concerning the Company, the price of shares of Marriott's securities declined precipitously and the Company was harmed and damaged as a direct and proximate result of its purchases of shares of Marriott's securities at artificially inflated prices and the subsequent decline in the price of shares of those securities when such facts were revealed.

592. By reason of the foregoing, the Officer Defendants and the Audit Committee

Defendants are liable to the Company as controlling persons of Marriott in violation of Section 20(a) of the Exchange Act.

**COUNT VI**

**(Against the Director Defendants for Violations of Section 14(a) of the Exchange Act)**

593. Plaintiffs incorporate by reference and re-alleges each and every allegation set forth above, as though fully set forth herein.

594. The Section 14(a) Exchange Act claims alleged herein are based solely on negligence. They are not based on any allegation of reckless or knowing conduct by or on behalf of Defendants. The Section 14(a) claims alleged herein do not allege and do not sound in fraud. Plaintiffs specifically disclaim any allegations of, reliance upon any allegation of, or reference to any allegation of fraud, scienter, or recklessness with regard to these nonfraud claims.

595. Section 14(a) of the Exchange Act, 15 U.S.C. § 78n(a)(1), provides that "[i]t shall be unlawful for any person, by use of the mails or by any means or instrumentality of interstate commerce or of any facility of a national securities exchange or otherwise, in contravention of such rules and regulations as the [SEC] may prescribe as necessary or appropriate in the public interest or for the protection of investors, to solicit or to permit the use of his name to solicit any proxy or consent or authorization in respect of any security (other than an exempted security) registered pursuant to section 12 of this title [15 U.S.C. § 78l]."

596. Rule 14a-9, promulgated pursuant to § 14(a) of the Exchange Act, provides that no proxy statement shall contain "any statement which, at the time and in the light of the circumstances under which it is made, is false or misleading with respect to any material fact, or which omits to state any material fact necessary in order to make the statements therein not false or misleading." 17 C.F.R. §240.14a-9.

597. Under the direction and watch of the Director Defendants, the 2017 Proxy Statement and 2018 Proxy Statement both failed to disclose that: (1) the Company did not maintain customer's personal data on a secure system; (2) unknown actors had gained unauthorized access to Starwood's network since 2014; (3) Marriott's due diligence in the Merger failed to discover the Data Breach; (4) the Data Breach caused personal information of up to 500 million guests to be exposed; (5) the Company failed to maintain internal controls; and (6) as a result of the foregoing the Company's public statements were materially false and misleading at all relevant times.

598. The Director Defendants also caused the 2017 Proxy Statement and 2018 Proxy Statement to be false and misleading with regard to executive compensation in that they purported to employ "pay-for-performance" elements while failing to disclose that the Company's stock price was being artificially inflated by Defendants' false and misleading statements and repurchases of Company stock, and therefore any compensation based on the Company's stock price was artificially inflated.

599. The 2018 Proxy Statement further described management's performance in integrating Starwood and Marriott as "outstanding" and the integration process as "seamless," assertions that were false and misleading in light of the ongoing Data Breach.

600. In the exercise of reasonable care, the Director Defendants should have known that by misrepresenting or failing to disclose the foregoing material facts, the statements contained in the 2017 Proxy Statement and 2018 Proxy Statement were materially false and misleading. The misrepresentations and omissions were material to Plaintiffs in voting on the matters set forth for shareholder determination in the 2017 Proxy Statement and 2018 Proxy Statement, including but not limited to, election of directors and the approval of officer compensation.

601. The false and misleading elements of the 2017 Proxy Statement led to the re-election of Defendants Sorenson, J.W. Marriott, Duncan, Harrison, Henderson, Hippeau, Kellner, Lee, Lewis, Muñoz, Reinemund, and Schwab allowed them to continue breaching their fiduciary duties to Marriott.

602. The false and misleading elements of the 2018 Proxy Statement led to the re-election of Defendants Sorenson, J.W. Marriott, Duncan, Harrison, Henderson, Hippeau, Kellner, Lee, Lewis, Muñoz, Reinemund, and Schwab allowed them to continue breaching their fiduciary duties to Marriott.

603. The Company was damaged as a result of Defendants' material misrepresentations and omissions in the 2017 Proxy Statement and 2018 Proxy Statement.

604. Plaintiffs, on behalf of Marriott, have no adequate remedy at law.

## XX. REQUEST FOR RELIEF

**WHEREFORE**, Plaintiffs demand judgment as follows:

A. Determining that this action is a proper derivative action maintainable under law, and that demand is excused;

B. Awarding, against all Defendants and in favor of the Company, the damages sustained by the Company as a result of Defendants' breaches of their fiduciary duties;

C. Directing the Company to take all necessary actions to reform and improve its corporate governance and internal procedures, to comply with the Company's existing governance obligations and all applicable laws and to protect the Company and its investors from a recurrence of the damaging events described herein;

D. Awarding to Plaintiffs the costs and disbursements of the action, including reasonable attorneys' fees, accountants' and experts' fees, costs, and expenses; and

E. Granting such other and further relief as the Court deems just and proper.

## XXI. JURY DEMAND

Plaintiffs demand a trial by jury.

Dated: August 21, 2020

Respectfully submitted,

*/s/ Gregory M. Egleston*
Gregory M. Egleston (admitted *pro hac vice*)
Robert J. Schupler (admitted *pro hac vice*)
**GAINEY McKENNA & EGLESTON**
501 Fifth Avenue, 19th Floor
New York, NY 10017
Telephone: (212) 983-1300
Facsimile: (212) 983-0380
Email: gegleston@gme-law.com
Email: rschupler@gme-law.com

***Co-Lead Counsel for Plaintiffs***

*/s/ Timothy Brown*
Timothy Brown (admitted *pro hac vice*)
**THE BROWN LAW FIRM, P.C.**
240 Townsend Square
Oyster Bay, NY 11771
Telephone: (516) 922-5427
Facsimile: (516) 344-6204
Email: tbrown@thebrownlawfirm.net

***Co-Lead Counsel for Plaintiffs***

*/s/ Andrew K. O'Connell*
Andrew K. O'Connell (Bar No. 28168)
**MURPHY, FALCON & MURPHY**
One South Street, 30th Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599
Email: andrew.oconnell@murphyfalcon.com

***Liaison Counsel for Plaintiffs***